RIKTLINJE

Informationssäkerhet

”Riktig information ska finnas tillgänglig för behörig personal på ett spårbart sätt när den behövs.”

1 INNEHÅLLSFÖRTECKNING

1 Innehållsförteckning 2

2 Inledning och omfattning 5
2.1 Inledning 5
2.1.1 processinriktning 6
2.2 Roller 7
2.2.1 Strategisk nivå 7
2.2.2 Budgetnivå (Taktisk nivå) 8
2.2.3 Beslutsnivå (Taktisk nivå) 9
2.2.4 Operativ nivå 10
2.3 Avgränsningar 11
2.4 Stadens styrande dokument 11

3 Definitioner 12

4 Riskbedömning och riskbehandling 13
4.1 Bedömning av säkerhetsrisker 13
4.2 Hantering av säkerhetsrisker 14

5 Säkerhetsprogram 15
5.1 uppföljning av riktlinjer för Informationssäkerhetsarbetet 16

6 Organisation av informationssäkerheten 16
6.1 Intern organisation 17
6.1.1 informationssäkerhetsorganisation vid förvaltningar och bolag 17
6.1.2 ledningens ansvar för informationssäkerheten 18
6.1.3 samordning av informationssäkerhetsarbetet 18
6.1.4 process för godkännande av Informationsbehandlingsresurser 18
6.1.5 sekretessförbindelse 18
6.1.6 Utomstående parter 18

7 Hantering av tillgångar 19
7.1 Ansvar för tillgångar 19
7.2 Klassificering av information 19
7.2.2 märkning och hantering av information 19

8 Personal och säkerhet 21
8.1 Säkerhet vid rekrytering för anställd och inhyrd personal 21
8.1.1 krav på anställda gällande informationssäkerhet 22
8.2 Regler för vissa system 22
8.2.1 Privat användning av Stockholm stads IT-system 22
8.2.2 e-postregler 23
8.2.3 internetanvändning 24
8.2.4 utbildning i informationssäkerhet 24

9 Fysisk och miljörelaterad säkerhet 25
9.1 Säkrade utrymmen 25
9.1.1 skalskydd och tillträde 25
9.2 Skydd av utrustning 26
9.2.1 fysiskt skydd, elförsörjning och kablageskydd 26

9.2.2 publika miljöer *27*
9.2.3 säkerhet för utrustning utanför egna lokaler *28*

10 Styrning av kommunikation och drift 28
10.1 Driftrutiner och driftansvar 28
10.1.1 dokumenterade driftrutiner *28*
10.1.2 styrning av ändringar i driftmiljö *28*
10.2 Systemplanering och systemgodkännande 29
10.2.1 driftgodkännande *29*
10.3 Skadlig kod 30
10.3.1 skydd mot skadlig kod *30*
10.4 Säkerhetskopiering 31
10.4.1 säkerhetskopiering *31*
10.5 Styrning av nätverk 32
10.5.1 nätverk *32*
10.6 Mediahantering och mediasäkerhet 33
10.6.1 hantering av flyttbara media *33*
10.6.2 avveckling av media *33*
10.6.3 säkerhet för systemdokumentation *34*
10.7 Utbyte av information och program 34
10.7.1 annat informationsutbyte *34*
10.8 Elektroniskt offentliggjord information 35
10.9 Övervakning 35
10.9.1 loggar *35*

11 Styrning av åtkomst 36
11.1 Verksamhetskrav på styrning av åtkomst 36
11.1.1 åtkomst *36*
11.2 Styrning av användares åtkomst 36
11.2.1 behörighetsadministration *36*
11.2.2 lösenordsregler *38*
11.2.3 behörighetskontroll *38*
11.3 Styrning av åtkomst till nätverk 39
11.3.1 utnyttjande av nätverkstjänster *39*
11.4 Styrning av åtkomst till operativsystem 40
11.4.1 åtkomst till operativsystem *40*
11.5 Styrning av åtkomst till information och tillämpningar 40
11.5.1 åtkomst till information och verksamhetssystem *40*
11.6 Mobil datoranvändning och distansarbete 41
11.6.1 mobil datoranvändning *41*
11.6.2 distansarbete *42*

12 Systemutveckling/-inköp och systemunderhåll 43
12.1 Säkerhetskrav på IT-system 43
12.1.1 analys och specifikation av säkerhetskrav *44*
12.2 Säkerhet i tillämpningar 45
12.2.1 informationskvalitet *45*
12.2.2 elektronisk signatur *45*
12.3 Kryptering 45
12.3.1 krypteringsregler *45*
12.4 Säkerhet i databaser och program 46
12.4.1 styrning av säkerhet i databaser och program *46*
12.5 Skydd av testdata 46

13 Hantering av informationssäkerhets-Incidenter 46
13.1 Säkerhetsincidenter och funktionsfel 46
13.1.1 rapportering 46
14 Kontinuitets- och avbrottsplanering 47
14.1 Kontinuitetsplanering 47
14.1.1 processen kontinuitetsplanering 47
14.2 Avbrottsplanering 48
14.2.1 processen avbrottsplanering 48
14.3 Riskanalyser 49
14.3.1 processen riskanalys 49
15 Efterlevnad 50
15.1 Identifiering av tillämpliga bestämmelser 50
15.1.1 lagar och förordningar 50
15.1.2 immaterialrätt 50
15.1.3 skydd av personuppgifter 50
15.2 Granskning av säkerhetspolicy, etik och teknisk efterlevnad 51
15.2.1 kontroll av säkerhetspolicy och etik 51
15.2.2 kontroll av teknisk efterlevnad 52
15.3 Hänsynstaganden vid revision av IT system 52
15.3.1 styrning av revision av it-system 52

2 INLEDNING OCH OMFATTNING

2.1 Inledning

Information, personal och ekonomiska tillgångar är några av Stockholms stads viktigaste resurser.

Stockholms stad förfogar över mycket stora mängder information som är skapad, lagrad, förvarad och bearbetad genom århundraden. Kunskap och kompetens hos stadens medarbetare är en annan informationskälla. Den information som staden ansvarar för måste skyddas vare sig den finns i historiska dokumentsamlingar, är lagrad i informationssystem eller är muntligt förmedlad.

Hot mot stadens information förekommer i olika former. Bränder, vattenläckage, stölder, förfalskning och bedrägerier är bara några exempel. IT och Internet har blivit en arena för försäljning av varor, hot och utpressningar, stölder och bedrägerier. Kort sagt samma sorts kriminalitet som finns utanför den digitala världen.

IT har förändrats från att ha varit ett stöd för, till att ha blivit en förutsättning för verksamheterna. Det är därför viktigt att den som har ett verksamhetsansvar också identifierar beroendet av IT för att kunna fullgöra sina åtagande även vid en kris, katastrof eller när informationssystemen inte fungerar.

Allmänhetens rättighet till insyn i den kommunala förvaltningen är ytterligare en orsak till att hålla god ordning på vår information.

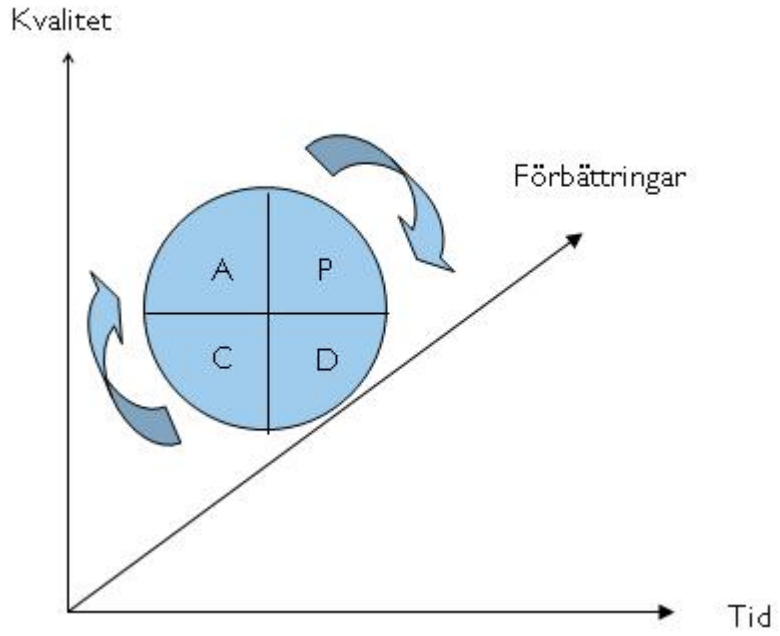
Informationssäkerhet handlar om hur staden ska minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information staden har en skyldighet att skydda

Dessa riktlinjer anger vad och hur verksamheterna ska agera för att initiera, införa, bibehålla och förbättra informationssäkerheten i staden. Riktlinjerna ska ses som ett lägsta krav vid utveckling eller inköp av nya system och målet för redan driftsatt system.

Irene Lundquist Svenonius
stadsdirektör

2.1.1 PROCESSINRIKTNING

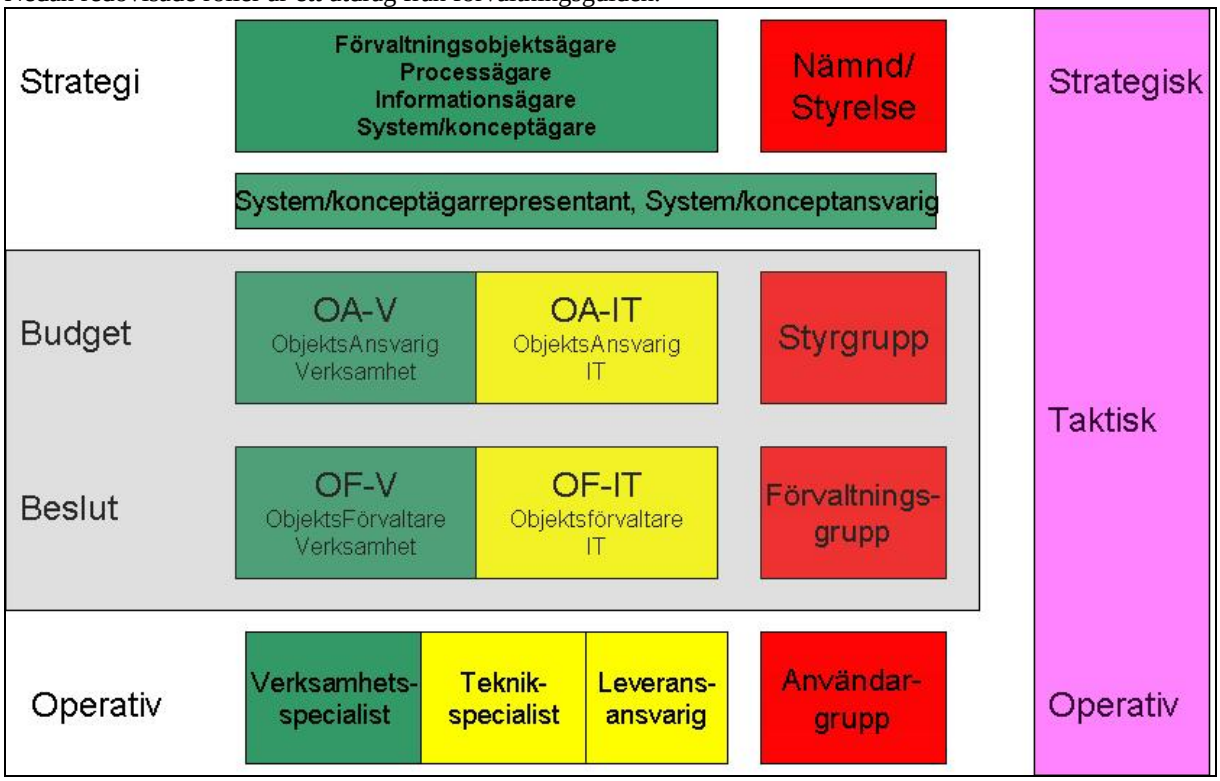
PDCA (Plan Do Check Act) utgör grunden för informationssäkerhetsarbetet i Stockholms stad. Det bygger på att verksamheten, IT och säkerheten arbetar processorienterat för att upprätthålla och förbättra kvaliteten såväl i verksamheten som i informationssäkerhetsarbetet. Målet är att uppnå ständiga förbättringar.



P, Plan (planera) Planera för att införa säkerhetshöjande åtgärder	**D, Do (genomföra)** Genomför de säkerhetshöjande åtgärderna
C, Check (kontrollera) Kontrollera att målen med de säkerhetshöjande åtgärderna uppfylls	**A, Act (agera)** Analysera och utvärdera införandet. Ta fram förslag på nya säkerhetshöjande åtgärder

2.2 Roller

Nedan redovisade roller är ett utdrag från förvaltningsguiden.



2.2.1 STRATEGISK NIVÅ

Roll	Beskrivning
Förvaltningsobjektsägare **Processägare** **Informationsägare** **System-/Konceptägare** **(Verksamhet)**	Nämnder och styrelser ansvarar för att: - IT-verksamheten inom nämnden bedrivs med rätt krav på säkerhet, skydd av personlig integritet och förtroende hos allmänheten - hantering av personuppgifter sker i enlighet med Offentlighets- och sekretesslagen samt personuppgiftslagen - information som rör egen verksamhet i gemensamma system är korrekt - de regler och riktlinjer som utfärdas av kommuncentrala organ sprids, förstås och efterlevs inom förvaltningar och bolag - all berörd personal har tillräcklig utbildning och tydliga instruktioner för att genomföra sina arbetsuppgifter i samband med IT på ett effektivt och säkert sätt

2.2.2 BUDGETNIVÅ (TAKTISK NIVÅ)

Roll	Beskrivning
Objektansvarig verksamhet (OA-V) (Verksamhet)	**Ansvar och befogenheter** • Att objektverksamheten har behovsanpassade förvaltningstjänster tillgängliga i syfte att omsätta IT:s nyttoeffekter i verksamheten • Att förvaltningsobjektet följer gällande lagar och interna styrdokument • Att förvaltningsobjektet har en aktuell förvaltningsplan • Att förvaltningsorganisationens effektivitet utvärderas periodiskt **Befogenhet** • Regleras av gällande delegations- och attestordning **Arbetsuppgifter** • Fastställa förvaltningsplanen tillsammans med OA-IT • Bemanna OF-V rollen samt ordförande i styrgrupp • Säkerställa att relevanta styrdokument kommer till OF-V:s kännedom
Objektansvarig IT (OA-IT) (IT)	**Ansvar** • Att tillgodose verksamhetsbehov av IT-tjänster enligt ställda krav • Att IT-tjänster följer gällande lagar och förordningar (t ex IT-säkerhetsregler och IT-strategier) **Befogenhet** • Regleras av gällande delegations- och attestordning **Arbetsuppgifter** • Tillsammans med OA-V fastställa förvaltningsplanen • Bemanna OF-IT rollen och delta i styrgruppsmöten • Följa upp avtal med kontrakterade IT-leverantörer i enlighet med förvaltningsplan • Säkerställa att relevanta styrdokument kommer till OF-IT:s kännedom

Styrgrupp	**Styrgruppen ska bemannas med:** • Verksamhetsansvariga som representerar verksamheterna inom system- eller konceptområdet (alternativt representanter utsedda av verksamhetsansvariga). • System-/konceptansvarig **Ansvar och befogenheter** Styrgruppens syfte/ inriktning är: • rådgivande grupp • prioritera aktiviteter avseende system-/koncept inom samma område • Strategisk styrning av förvaltningen ur ett verksamhetsperspektiv. **Exempel på arbetsuppgifter kan vara att:** • godkänna projektets leveranser • ta emot projektets slutrapport • ha verksamhetsansvar för projektresultatet.

2.2.3 BESLUTSNIVÅ (TAKTISK NIVÅ)

Roll	Beskrivning
Objektförvaltare Verksamhet (OF-V) (Verksamhet)	Den roll på förvaltningsorganisationens beslutsnivå som ansvarar för att målen i förvaltningsplanen uppnås samt att uppföljning och avvikelser rapporteras till styrgrupp. Ingår i förvaltningsgruppen.
Objektförvaltare IT (OF-IT) (IT)	Den roll på förvaltningsorganisationens beslutsnivå som har till ansvar att säkerställa det fortlöpande IT-stödet till verksamheten enligt målen i förvaltningsplanen. Ingår i förvaltningsgruppen.
Förvaltningsgrupp	**Förvaltningsgruppen bemannas med:** • Objektansvarig verksamhet och objektansvarig IT samt • Ytterligare personer som kan vara viktiga t ex roller från användargrupp. **Ansvar och befogenheter** • Tar fram underlag till förvaltningsplan samt • Prioriterar och beslutar om förvaltningsaktiviteter inom ramarna för förvaltningsplanen och rapporterar uppföljning och avvikelser till styrgrupp. **Arbetsuppgifter:** Fungerar som arbetsgrupp för det löpande förvaltningsarbetet

2.2.4 OPERATIV NIVÅ

Roll	Beskrivning
Verksamhetsspecialist (VS) (Verksamhet)	Verksamhetsspecialister är resurser som utför verksamhetsnära förvaltningsaktiviteter, främst användarstöd och ändringshantering, på uppdrag av OF-V. **Exempel på arbetsuppgifter:** • utarbeta funktionsspecifikationer för ändringar • genomför tester av ändringar • administrerar utbildningsaktiviteter • administrerar och genomför informationsaktiviteter
Leveransansvarig (LA) (IT)	Leveransansvariga representerar respektive kontrakterad IT-leverantör i förvaltningsverksamheten och utgör kontaktytan mellan förvaltningsorganisationen och IT-leverantören i frågor gällande förvaltningsplanens verkställande . **Ansvar:** • Att säkerställa aktuell IT-leverans och att den tillgodoser de krav som staden ställt **Arbetsuppgifter:** • säkerställa att de förvaltningsaktiviteter som överenskommits i förvaltningsplanen genomförs av resurser hos IT-leverantören • medverkar vid uppföljning av förvaltningsplan och avtal gällande IT-leverantörens åtagande • hanterar avvikelser från överenskommen IT-leverans gentemot IT-leverantören
Tekniкspecialist (TS) (IT)	Tekniкspecialister är resurser som utför IT-nära förvaltningsaktiviteter, främst användarstöd och ändringshantering, på uppdrag av OF-IT. **Exempel på arbetsuppgifter:** • samordnar tester och produktionssättning av ändringar i IT-tjänsterna • granskar och upprätthåller systemdokumentation • administrerar och genomför utbildningsaktiviteter gentemot IT-parter • administrerar och genomför informationsaktiviteter gentemot IT-parter

Roll	Beskrivning
Användargrupp	Förekommer vid behov. Denna grupp utses av objektansvarig verksamhet /IT (OA-V/OA-IT) eller objektförvaltare verksamhet/IT (OF-V/OF-IT) i samråd med verksamheten. • Bemanningen ska vara representativ för förvaltningsobjektets användare. • Sammankallande är OF-V eller OF-IT. • Detta är en rådgivande grupp för prioritering och förankring av förändringar i förvaltningsobjektet samt spridning av information. Representant i användargrupp ska vara verksamhetens kanal för krav och ändringsbehov inom förvaltningsobjektet **Ansvar och befogenheter** • Att ge användarna det stöd som specificerats i förvaltningsavtalet • Kan ta emot och administrera problemrapportering • Förmedla problemrapportering till objektförvaltare • Ge ändringsförslag till objektförvaltare • Se till att systemanvändarna får uppdaterad användardokumentation och annan för systemet nödvändig information.

2.3 Avgränsningar

Riktlinjerna reglerar inte hanteringen av sekretessbelagda uppgifter enligt Offentlighets- och sekretesslagen (2009:400) 15 kap 2§ (försvarssekretess) i våra informationssystem.

2.4 Stadens styrande dokument

Dokument	Diarienummer
Säkerhetsprogram för Stockholms stad	307-2883/2008
E-Strategi	051-823/2008
IT-program	031-2486/2007
Informationsteknisk plattform (ITP)	055-1611/2001

3 DEFINITIONER

Begrepp	**Beskrivning**
Autenticering	Verifiering av uppgiven identitet.
Avbrottsplan (IT)	Plan för hur driften ska återupptas efter driftstörning eller då IT-system inte fungerar som de ska. Avbrottsplanen baseras på kontinuitetsplanen.
Identitet	Unik beteckning för en viss användare.
Incident	Säkerhetshändelse som kan/kunnat få/har fått allvarliga konsekvenser för verksamheten.
Informationsklassificering	Ett formellt sätt att fastställa rätt skyddsnivå för ett IT-system. Uttrycks i en s.k. säkerhetsprofil.
Informationstillgångar	En organisations skyddsvärda informationsrelaterade tillgångar. *Exempel på informationstillgångar är:* *Information (databaser, filer, metodik, dokument, etc.)* *Program (tillämpningar, operativsystem, etc.)* *Tjänster (nätförbindelser, abonnemang, etc.)* *Fysiska tillgångar (datorer, datamedia, lokala nätverk, etc.)*
IT-system	Består av datorer, tillbehör, minnesenheter, program, kommunikationsutrustningar, metoder och procedurer som har till uppgift att genomföra elektronisk behandling av information.
Kontinuitetsplan (för verksamheten)	Planen beskriver hur verksamheten ska bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas av störning under en längre, specificerad tidsperiod.
Logg	Information om de operationer som utförs i ett IT-system. Tre typer av loggar är aktuella: Säkerhetslogg, systemlogg och transaktionslogg.
Riktighet	Åtgärder för att åstadkomma rätt kvalitet i informationen.
Risk	Sannolikheten för en skadlig händelse multiplicerat med konsekvensen av skadan.
Riskanalys	Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.
Sekretess	Skydd mot obehörig åtkomst av information. (Förbud att röja uppgift vare sig det sker muntligt eller att handlingen lämnas ut.) Begreppet ersätts med Åtkomstbegränsning i detta dokument.
SLA (Service Level Agreement)	Dokument som reglerar vad som överenskommits mellan objektsansvarig och IT-leverantör om drift och förvaltning av

	visst IT-system.
Spårbarhet	Möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse.
Systemlogg	Loggfil som innehåller händelser utförda av systemkomponenter i operativsystemet. t ex om en drivrutin eller någon annan systemkomponent inte kan läsas in när programmet startas, loggas detta i systemloggen. Händelsetyperna som loggas av systemkomponenter är förbestämda operativsystemet.
Sårbarhet	Brist i skyddet av en tillgång som är utsatt för ett hot.
Säkerhet	Säkerhet innebär skydd mot och förmåga att hantera konsekvenser av oönskade händelser och dess skadliga effekter på människor, egendom och miljö inom stadens ansvarsområden.
Säkerhetslogg	Loggfil som innehåller händelser om giltiga och ogiltiga inloggningsförsök och händelser som har anknytning till resursanvändning, t ex att skapa, öppna eller ta bort filer eller andra objekt.
Säkerhetsprofil	Alla IT-system har ett skyddsbehov. Genom att klassificera informationen utifrån åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet får vi en säkerhetsprofil. Den avgör vilka säkerhetskrav som ska ställas på informationstillgången.
Tillgänglighet	Åtgärder för att säkra drift och funktionalitet.
Transaktionslogg	Loggfil som innehåller händelser i ett ekonomisystem t ex vem som attesterat vilket belopp vid vilken tidpunkt etc.
Åtkomst-/behörighetskontroll	Den ska reglera och kontrollera en användares åtkomst till olika informationstillgångar samt skydda information och program så att de endast är tillgängliga utifrån tilldelad (roll-)behörighet.

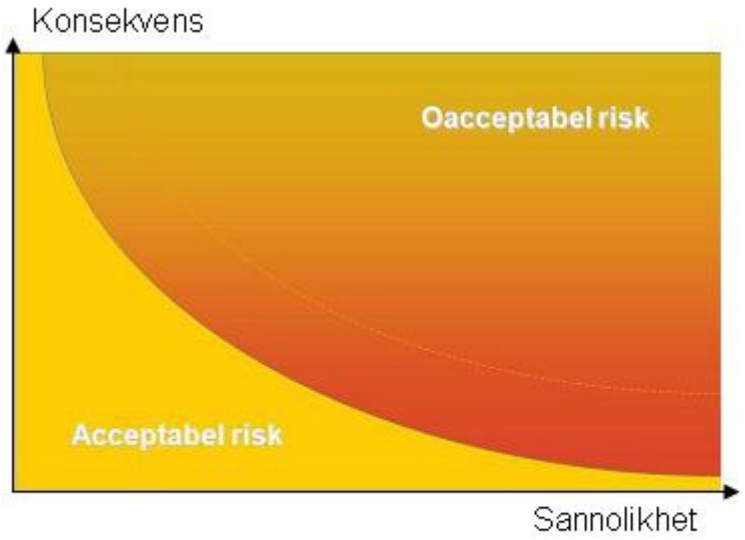
4 RISKBEDÖMNING OCH RISKBEHANDLING

4.1 Bedömning av säkerhetsrisker

En säkerhetsrisk är summan av sannolikheten för att något ska inträffa och konsekvensen av det inträffade.

Stockholms stad har utarbetat en modell för hur riskanalysen ska genomföras. Stadsledningskontorets säkerhetschef eller informationssäkerhetschef kan bistå med ytterligare information. Det är inte enbart informationssystem som ska analyseras utifrån modellen utan även viss verksamhet. Riskanalysen ska ge svar på följande frågor:

VAD kan gå fel?
HUR sannolikt är detta?
HUR stor blir skadan (konsekvenser)?



Riskanalysen ska revideras när verksamheten eller förutsättningarna för verksamheten väsentligt förändras.

4.2 Hantering av säkerhetsrisker

De risker som identifieras i riskanalysen ska hanteras. Det görs genom att:

- Genomföra åtgärder som minskar riskerna till en acceptabel nivå.
- Acceptera riskerna om de inte strider mot lagstiftning, stadens regler eller stadens kriterier för riskacceptans.
- Undvika aktiviteter som kan orsaka att identifierade risker uppstår.
- Överföra risken till andra parter, t.ex. försäkringsbolag eller leverantörer.

4.2.1.1 Anvisningar för hur säkerhetsrisker ska hanteras

Alla system och verksamheter har risker. Därför ska en risk- och sårbarhetsanalys (RSA) genomföras för att kunna identifiera och prioritera riskerna.

- Om en risk för lagöverträdelse identifieras ska den åtgärdas före driftsättning. Om en lagöverträdelse i ett redan driftsatt system identifieras ska detta stoppas omedelbart.
- När åtgärderna som krävs för att minska en risk inte är ekonomiskt försvarbara eller om åtgärderna är så omfattande att ett införande inte är praktiskt möjligt kan beslut om riskacceptans fattas. Detta görs av behörig delegat på initiativ av styrgrupp. Ett riskacceptansbeslut måste innehålla:
    - Datum för beslutet
    - Beslutets giltighetstid
    - Vem som har fattat beslutet
    - Vem som har föredragit ärendet
    - Beskrivning av risken som accepteras
    - Motiv till beslutet

5 SÄKERHETSPROGRAM

Säkerhetsprogram för Stockholms stad (Dnr 307-2883/2008) innehåller bland annat stadens planering för informationssäkerheten:
”Med informationssäkerhet avses alla aktiviteter som syftar till bevarandet av konfidentiella uppgifter, riktighet och tillgängligheten hos information. Andra egenskaper t. ex. autencitet, spårbarhet, oavvislighet och tillförlitlighet kan också rymmas i begreppet informationssäkerhet. Stadens planering för informationssäkerhetsarbetet är att all information vare sig den finns lagrad digitalt, på papper eller är muntligt förmedlad ges ett adekvat skydd. Detta för att ***riktig information ska finnas tillgänglig för behörig personal på ett spårbart sätt när den behövs***.

Säkerhetsarbetet omfattar alla åtgärder vars samlade effekt är att förebygga och begränsa konsekvenserna av störningar för informationshantering inom stadens verksamheter. Personer som omfattas är förtroendevalda, anställda och i viss omfattning skolelever samt konsulter/entreprenörer om uppdragens karaktär är relevanta för informationssäkerheten. Informationssäkerhet ska vara en integrerad del av allt arbete i staden. Alla som i någon utsträckning hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten.”

Informationssäkerhet handlar om:
Åtkomstbegränsning (Sekretess) – skydd mot obehörig åtkomst av information
Riktighet – åtgärder för att åstadkomma rätt kvalitet på information
Tillgänglighet – åtgärder för att säkra drift och funktionalitet
Spårbarhet – möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse

Stadens informationssäkerhetsorganisation ska vara känd och berörd personal ska ha nödvändiga kunskaper om aktuella IT-stöd och säkerhetsregler.
Ansvariga: Verksamhetsansvarig chef

Säkerhetsaspekterna ska uppmärksammas vid utveckling och inköp av system. Skriftligt godkända servicenivåer ska finnas före driftsättning. Kontinuitetsplan ska finnas för verksamheter med starkt beroende av verksamhetssystem och IT-stöd.
Tillämpning av stadens riktlinjer för informationssäkerhet innebär att:

- Grundnivån för säkerheten ska fastställas genom informationsklassificering
- Riskanalys ska genomföras för att kostnaden för skyddet ska stå i proportion till värdet av informationen
- Åtkomst/behörighet ska tilldelas formellt och endast efter behov samt följas upp regelbundet
- Alla incidenter ska rapporteras och kontinuerlig uppföljning ska ske mot fastställda regler.

Den som använder Stockholms stads informationstillgångar på ett sätt som strider mot riktlinjerna blir föremål för åtgärder från stadens sida. Genom att följa handlingsplaner och genomföra de åtgärder som beskrivs i stadens regelverk kan informationssäkerhetsarbetet förverkligas. Regler och riktlinjer och fortsatt utveckling av informationssäkerhetens praktiska hantering fastställs i riskhanteringsrådet.

5.1 uppföljning av riktlinjer för Informationssäkerhetsarbetet

Riktlinjerna för informationssäkerhetsarbetet ska granskas och revideras varje år för att se om betydande förändringar inträffat inom staden, för att säkerställa att planen fortfarande är relevant och inte står i strid med lagstiftningen och att planen följer den tekniska utvecklingen.
Ansvarig: Informationssäkerhetschef

6 ORGANISATION AV INFORMATIONSSÄKERHETEN

Till stöd för stadens säkerhetsarbete och för Kommunfullmäktiges mål om en trygg och säker stad finns ett strategiskt riskhanteringsråd. Informationssäkerhetsfrågorna är integrerade i rådets arbete.

Informationssäkerhetschefen som är placerad på stadsledningskontoret samordnar stadsövergripande aktiviteter och verkar som rådgivare för förvaltningar och bolag.

6.1 Intern organisation

6.1.1 INFORMATIONSSÄKERHETSORGANISATION VID FÖRVALTNINGAR OCH BOLAG

Informationssäkerhetsarbetet i förvaltningar och bolag leds av en informationssäkerhetssamordnare.
Förvaltningar och bolag beslutar själva om utformningen av den egna säkerhetsorganisationen. Säkerhetssamordnare och informationssäkerhetssamordnare måste dock alltid finnas, och om uppgifter behandlas i verksamheten som rör rikets säkerhet ska även en säkerhetsskyddssamordnare finnas.

Informationssäkerhetssamordnare

Informationssäkerhetsarbetet vid förvaltningar och bolag leds av en utsedd informationssäkerhetssamordnare. Informationssäkerhetssamordnaren ska ha kunskap om stadens informationssäkerhetsregler, stadens säkerhetsarbete och kunna bistå med kompetens vid t ex informationsklassificeringar samt risk och sårbarhetsanalyser. Andra uppgifter kan vara att:

- sprida information och kunskap om stadens informationssäkerhetsarbete inom förvaltning/bolag
- vara kontaktperson mot stadens informationssäkerhetschef
- se till att nödvändiga instruktioner utformas och beslutas
- samordna och följa upp informationssäkerhetsarbetet
- rapportera allvarliga incidenter till stadens informationssäkerhetschef

Informationssäkerhetsresurs

Om ytterligare informationssäkerhetskompetens behövs inom förvaltningen eller bolaget kan ytterligare personer med informationssäkerhetsarbetsuppgifter utses. De hjälper till att upprätthålla informationssäkerheten inom den egna enheten, t.ex. en skola. Syftet med att ha informationssäkerhetsresurs är att de kan säkerställa att regelverk och planer verkställs och efterlevs. De kan även vara ett nära stöd till verksamhetsansvariga chefer inom informationssäkerhetsområdet.
Exempel på uppgifter för en informationssäkerhetsresurs:

- Ge råd i informationssäkerhetsfrågor på arbetsplatsen.
- Stödja verksamhetschefen med att ta fram planer och genomföra utbildningar

Informationssäkerhetsansvarig i särskilda projekt

För att övervaka att säkerhetsaspekterna i ett projekt omhändertas på ett tillfredsställande sätt bör en särskild informationssäkerhetsansvarig tillsättas. Erfarenheterna visar att det finns stora risker för förseningar och kostnadsökningar om inte säkerheten uppmärksammas i ett tidigt skede i projektet.

I uppgifterna ingår att:

- Se till att informationsklassificering genomförs

- Riskanalys genomförs
- Systemet testas

6.1.2 LEDNINGENS ANSVAR FÖR INFORMATIONSSÄKERHETEN

Förankringen och medvetandet hos medarbetarna utgör själva grunden för informationssäkerhetsarbetet. Därför är det ett ansvar för chefer på alla nivåer inom staden att kommunicera vikten av god informationssäkerhet. Informationssäkerhet är därför ett ansvar för chefer på alla nivåer inom staden.

Stadens nämnder och styrelser är ytterst ansvariga för informationssäkerheten genom att:

- Resurser avsätts för att möta de hot som kan uppstå i den egna verksamheten
- Oberoende granskningar genomförs av system och säkerhetslösningar som tagits fram av den egna organisationen
- Verksamheten följer stadens regler genom internkontroller

Som systemägare har nämnden/styrelsen även ett ekonomiskt, funktionellt och säkerhetsmässigt ansvar för sina informationssystem under hela dess livscykel.

6.1.3 SAMORDNING AV INFORMATIONSSÄKERHETSARBETET

Kommunstyrelsen har det stadsövergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjerna för informationssäkerheten.

6.1.4 PROCESS FÖR GODKÄNNANDE AV INFORMATIONSBEHANDLINGSRESURSER

Införandet av nya system ska följa stadens fastställda rutiner (Utvecklingsguide, Lilla och Stora ratten, Testhandboken m.fl.), vilket bl. a. innebär att informationsklassificering och riskanalys ska genomföras och att systemen ska testas innan de driftsätts. För att säkra kvaliteten i driften av stadens gemensamma IT-miljö har ett centralt ändringsråd (Change Advisory Board) inrättats. Ändringrådets uppgift är enkelt sammanfattat att ta ställning till om planerade förändringar i berörda IT-system förberetts på rätt sätt innan genomförande.

6.1.5 SEKRETESSFÖRBINDELSE

Den som i sin yrkesroll får ta del av sekretessbelagd information bör underteckna en sekretessförbindelse.

6.1.6 UTOMSTÅENDE PARTER

Avtal med utomstående parter ska reglera såväl den affärsmässiga och säkerhetsmässiga överenskommelsen. Säkerhetskrav som kommer att ställas på den utomstående ska redovisas.

7 HANTERING AV TILLGÅNGAR

7.1 Ansvar för tillgångar

Alla informationstillgångar, dyr och svårersättlig utrustning ska ha en ansvarig. Den ansvarige ska utfärda instruktioner om hur informationen och utrustningarna ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även vara märkta.

7.1.1.1 Anvisningar för förteckning och märkning av tillgångar

7.1.1.1-1	Informationstillgångar representerar stora värden och ska därför förtecknas. Förteckningarna ska hållas noggrant uppdaterade.
7.1.1.1-2	Ansvarig för informationstillgångar ska finnas utsedd
7.1.1.1-3	Utrustning, i synnerhet stöldbegärlig, ska vara märkt. Stöldskyddsmärkningen ska göras så att märkningen inte går att avlägsna utan svårighet.

7.2 Klassificering av information

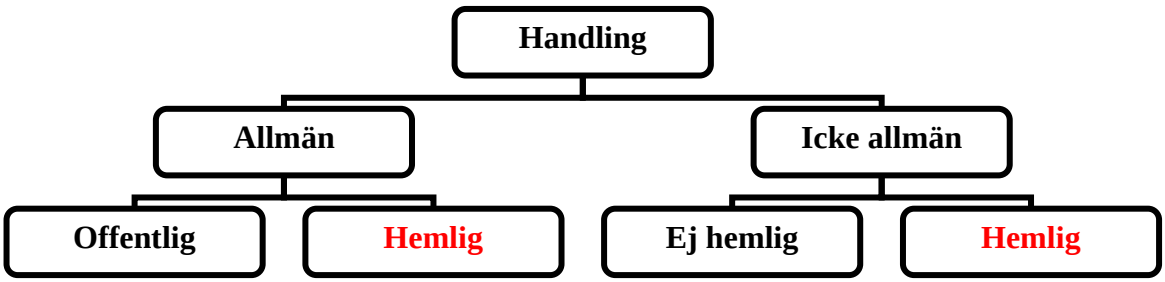
Alla stadens informationstillgångar ska vara klassificerade. Informationstillgångarna ska klassificeras (värderas) så att rätt skyddsnivå kan fastställas. Klassificering ska ske tidigt i samband med systemutveckling/-inköp men även i förvaltningsskedet. Klassificeringen utgår från faktorerna Åtkomstbegränsning, Riktighet, Tillgänglighet och Spårbarhet. Stadens fastställda metod för informationsklassificering ska användas.

7.2.1.1 Anvisningar för informationsklassificering

7.2.1.1-1	Informationstillgångarna ska klassificeras för att säkerställa att de ges ett tillräckligt skydd. Förutom lagliga krav på skydd ska verksamhetens bedömning av informationens värde avseende åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet avgöra omfattningen av det skydd som ska uppnås.
7.2.1.1-2	Informationsklassificering ska ske enligt Handbok för Informationsklassificering.

7.2.2 MÄRKNING OCH HANTERING AV INFORMATION

Information som är belagd med sekretess ska märkas så att detta framgår. Det ska även framgå om informationen är original eller kopia. Sekretessprövning ska alltid föregå beslut om utlämnande av information.
Hemlig information enligt Offentlighet och sekretesslagen 15 kap 2§ (förvarssekretess) hanteras inte i detta dokument.



Stadens informationshantering styrs främst av bestämmelser i tryckfrihetsförordningen och Offentlighet- och Sekretesslagen (OSL) 2009:400. Huvudregeln i tryckfrihetsförordningen är att informationen ska vara tillgänglig för allmänheten, den s k offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i OSL kan omfattas av sekretesskydd. Det är väsentligt att varje anställd känner till vilken information, inom i första hand sitt eget ansvarsområde, som är sekretessbelagd och hur den ska hanteras. Prövning av sekretess föreligger för viss information varje gång en begäran om utlämning sker. Detta oavsett om handlingen är sekretessbelagd eller inte.

7.2.2.1 Anvisningar för hantering av allmänna hemliga handlingar

7.2.2.1-1	Sekretessbelagda handlingar är undantagna offentlighetsprincipen och ska skyddas från obehörig åtkomst.
7.2.2.1-2	Sekretessbelagda handlingar ska märkas med särskild anteckning (sekretessmarkering) på handlingen eller, om handlingen är elektronisk, införs anteckningen i handlingen eller i det datasystem där den elektroniska handlingen hanteras.
7.2.2.1-3	Hur märkning ska ske framgår av Offentlighets- och sekretesslagen 5 kap 5§.
7.2.2.1-4	Sekretessbelagda handlingar ska förvaras i säkerhetsskåp. Säkerhetsskåp ska uppfylla Stöldskyddsföreningens norm SS 3492.
7.2.2.1-5	Sekretessbelagda handlingar ska vid gallring förstöras i dokumentförstörare
7.2.2.1-6	Sekretessbelagda handlingar ska distribueras med bud eller rekommenderat brev med mottagningsbevis.
7.2.2.1-7	Sekretessbelagda handlingar i elektronisk form ska distribueras med krypterad förbindelse eller med filerna krypterade.
7.2.2.1-8	Sekretessbelagda handlingar i elektronisk form ska, om starkt behov av åtkomstbegränsning föreligger kunna lagras krypterade. Av staden rekommenderad lösning ska användas.
7.2.2.1-9	Sekretessbelagd handling som tas emot i elektronisk form får inte lagras i inkorgen utan ska omedelbart flyttas
7.2.2.1-10	Verksamhetsansvarig chef ska säkerställa att sekretessbelagda handlingar hanteras korrekt.

7.2.2.2 Anvisningar för hantering av allmänna offentliga handlingar

7.2.2.2-1	En handling anses som allmän, om den förvaras hos myndighet och är antingen inkommen till, eller upprättad hos myndighet.
7.2.2.2-2	All post som kommer utifrån ska gå via registraturet där den ska öppnas och bedömas om handlingen ska diarieföras.
7.2.2.2-3	Upprättade handlingar ska sekretessbedömas och registreras.
7.2.2.2-4	E-post, fax, SMS m.m. kan också vara en inkommen handling. Mottagaren bedömer om meddelandet ska diarieföras.
7.2.2.2-5	Avslutade ärenden ska arkiveras enligt gällande bestämmelser.
7.2.2.2-6	Alla handlingar ska sekretessbedömas, om möjligt av ansvarig handläggare innan de lämnas ut.

7.2.2.3 Anvisningar för hantering av icke allmänna handlingar

7.2.2.3-1	Minnesanteckningar, utkast, privata brev, underhandsremisser och koncept till en myndighets beslut är inte allmänna handlingar, om dessa inte expedierats eller tagits om hand för arkivering.
7.2.2.3-2	Samma regler gäller för icke allmänna hemliga handlingar som för allmänna hemliga handlingar.
7.2.2.3-3	I samband med resor, konferenser och motsvarande ska känsligt arbetsmaterial hanteras på sådant sätt att de inte exponeras för obehöriga.
7.2.2.3-4	För att spara lagringsutrymme på servrar bör icke allmänna handlingar raderas när de inte längre behövs.

8 PERSONAL OCH SÄKERHET

Genom säkerhetsinsatser ska riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar.

8.1 Säkerhet vid rekrytering för anställd och inhyrd personal

Vid rekrytering ska säkerhetsbestämmelserna beaktas. Platssökande ska kontrolleras på lämpligt sätt särskilt om anställningen medför åtkomst till sekretessbelagda uppgifter eller på annat sätt omfattar säkerhetskritiska aktiviteter. Information hur informationssäkerheten hanteras inom Stockholms stad ska lämnas till nyanställd personal.

8.1.1 KRAV PÅ ANSTÄLLDA GÄLLANDE INFORMATIONSSÄKERHET

8.1.1.1 Anvisningar för personal och säkerhet

8.1.1.1-1	Alla anställda ska vara medvetna om sitt ansvar för informationssäkerheten.
8.1.1.1-2	Vid nyanställning ska den anställde förbinda sig att ta del av och acceptera regelverket för informationssäkerhet. Detta sker lämpligen t ex när användarkontot kvitteras
8.1.1.1-3	Personal i viss verksamhet ska registerkontrolleras enligt gällande lagstiftning. För registerkontroll enligt Säkerhetsskyddslagen SFS 1996:627 hänvisas till stadens säkerhetsskyddschef vid stadsledningskontoret.
8.1.1.1-4	All personal ska ha kunskap om offentlighetsprincipen och om offentlighets- och sekretesslagen.
8.1.1.1-5	Lokala instruktioner som styr avveckling/förändring av åtkomst till såväl lokaler som IT-system ska finnas.
8.1.1.1-6	För personal med höga behörigheter till lokaler och IT-system och där uppsägning från arbetsgivarens sida eller där övertalighet är aktuell rekommenderas att behörigheterna för dessa personer omedelbart revideras.
8.1.1.1-7	Beställare/uppdragsgivare ska upprätta sekretessförbindelse för konsulter/entreprenörer med uppdrag inom staden innan uppdraget startar.
8.1.1.1-8	Vid tjänstledighet längre än sex månader ska, om inte annat överenskommits, åtkomsträttigheter till system revideras. Föräldralediga är undantagna.

8.2 Regler för vissa system

Det är under vissa förutsättningar tillåtet för stadens medarbetare att använda sin arbetsplatsutrustning även för privata angelägenheter.

8.2.1 PRIVAT ANVÄNDNING AV STOCKHOLM STADS IT-SYSTEM

8.2.1.1 Anvisningar för privat användning av Stockholm stads IT-system.

8.2.1.1-1	Användningen ska ske inom de ramar som sätts upp av lagar och förordningar och följa samma etiska normer som annan informationshämtning/ -spridning. Den får inte skada Stockholm stad anseende eller kränka någon enskild i eller utanför Stockholms stad.
8.2.1.1-2	Den privata användningen får inte vara av sådan omfattning att den inkräktar på användarens arbete.
8.2.1.1-3	Stadens utrustning får endast användas av den anställde.

8.2.1.1-4	Nedladdning och lagring av bild- film- och ljudfiler för privat bruk är inte tillåtet.
8.2.1.1-5	Användningen får inte innebära någon extra kostnad för staden.
8.2.1.1-6	Användaren ska vara medveten om att: - Meddelanden som skickas via e-post normalt inte är skyddade från insyn. - E-post som skickas till eller från Stockholm stads e-postadresser eller som finns i Stockholm stads IT-system kan uppfattas som stadens e-post. - Om en e-postadress lämnas till olika tjänster på Internet, t.ex. nyhetsbrev kan detta medföra att s.k. skräppost skickas tillbaka till e-postadressen. - Besök på webbplatser på Internet lämnar elektroniska spår efter sig. - Nätverkstrafik och dess innehåll loggas (registreras) och lagras.
8.2.1.1-7	Programvaror som inte är godkända av IT-chef eller motsvarande får inte förekomma i Stockholm stads IT-system.

8.2.2 E-POSTREGLER

8.2.2.1 Anvisningar för hantering av e-post

8.2.2.1-1	Varje nämnd har ett ansvar för att de allmänna handlingar som skapas i verksamheten hanteras enligt regelverket. Den har också ansvar för att alla anställda har kännedom om vilka regler som gäller.
8.2.2.1-2	Alla som använder e-post ska regelbundet kontrollera sin brevlåda.
8.2.2.1-3	E-post som är allmän handling ska registreras enligt föreskrifterna i Offentlighets- och Sekretesslagens 5 kapitel . Undantag gäller e-posthandlingar som uppenbart är av ringa betydelse för stadens verksamheter och för e-posthandlingar som på annat sätt görs sökbara och tillgängliga för utomstående.
8.2.2.1-4	Sekretessbelagda uppgifter får endast skickas med e-post till mottagare inom S:t Erik Net. Mottagaren ska omedelbart kunna flytta meddelandet från inkorgen. Sekretessbelagda och känsliga uppgifter får inte lagras i inkorgen
8.2.2.1-5	Handlingar i ett ärende ska alltid kunna presenteras tillsammans. Detta innebär att handlingar som kommit in eller upprättats elektroniskt bör tas ut på papper, om myndighetens aktsystem i övrigt är pappersbaserat.
8.2.2.1-6	De uppgifter om meddelandena som finns i loggar och andra förteckningar som genereras av systemet är allmänna handlingar och kan därmed bli tillgängliga.
8.2.2.1-7	De bestämmelser om bevarande och gallring av allmänna handlingar finns i arkivlagen samt i stadens arkivregler gäller även för e-posthantering.
8.2.2.1-8	Meddelanden som uppenbart är av ringa betydelse för nämndens verksamhet ska så snart som möjligt gallras (raderas) enligt nämndens tillämpningsbeslut med stöd av stadens allmänna gallringsregler. För gallring av övriga meddelanden krävs beslut av arkivmyndigheten.

8.2.2.1-9	Varje anställd ska ge fullmakt till en kollega som vid frånvaro kan ta hand om inkomna e-postmeddelanden. Det räcker inte med ett automatiskt svarsmeddelande om frånvaron.
8.2.2.1-10	Varje förvaltning ska ha en officiell e-postadress. Adressen publiceras externt, bl.a. på stadens webbplats. E-posten öppnas av registrator (eller motsvarande). Brevlådan ska vara tillgänglig för allmänheten, t.ex. hos registrator. Vid korrespondens med allmänheten ska det eftersträvas att använda den officiella adressen som avsändaradress. Det kan i många fall vara lämpligt att enheter/avdelningar eller särskilda verksamheter har en egen adress/brevlåda.
8.2.2.1-11	Sekretessbelagd information ska sändas krypterad. Detta medför bl.a. att e-post inte får vidarebefordras till externa adresser utan kontroll av förekomsten av sekretess.
8.2.2.1-12	Om e-postmeddelanden innehåller uppgifter om levande personer, ska personuppgiftslagens (1998:204) bestämmelser beaktas.
8.2.2.1-13	E-postsystemet får i begränsad omfattning användas för privata meddelanden. Användningen ska vara etiskt försvarbar.

8.2.3 INTERNETANVÄNDNING

8.2.3.1 Anvisningar för åtkomst till och användning av Internet

Internet är en av många informationskällor som används för att lösa arbetsuppgifter.

8.2.3.1-1	Använd Internet inom de ramar som sätts upp av lagar och förordningar, exempelvis Upphovsrättslagen och Personuppgiftslagen och följ samma etiska normer som för annan informationshämtning/ -spridning.
8.2.3.1-2	Material som är sekretessbelagt får inte publiceras på Internet.
8.2.3.1-3	Ladda aldrig ner musik-, film- eller programfiler för privat bruk.
8.2.3.1-4	Kontroll av respektive förvaltnings eller bolags surfning ska ske genom stickprov eller på annat vis.

8.2.4 UTBILDNING I INFORMATIONSSÄKERHET

Verksamhetsansvarig chef ansvarar för att berörd personal utbildas i informationssäkerhet.

8.2.4.1 Anvisningar för användarutbildning

Utbildning ska ges kontinuerligt för att skapa medvetande om informationssäkerhet och andra säkerhetskrav.

8.2.4.1-1	Objektsansvarig ska definiera vilka krav som ställs på systemets användare.
8.2.4.1-2	Alla användare, även konsulter och övriga tredjepartsanvändare, ska få en anpassad utbildning i informationssäkerhet.
8.2.4.1-3	Informationssäkerhetsbestämmelserna ska finnas tillgänglig för alla användare på stadens intranät. Ansvarig: Informationssäkerhetschefen

9 FYSISK OCH MILJÖRELATERAD SÄKERHET

9.1 Säkrade utrymmen

Åtgärder ska vidtas för att förhindra att obehöriga får tillträde till utrymmen med informationstillgångar. Åtgärder ska även vidtas för att förhindra skador och störningar där tillgångarna är placerade.

9.1.1 SKALSKYDD OCH TILLTRÄDE

För verksamheten kritiska eller viktiga informationstillgångar ska förvaras i säkrade utrymmen inom ett avgränsat skalskydd med lämpliga spärrar och tillträdeskontroller. Nivån på skalskyddet fastställs med hjälp av riskanalys.
För att upprätthålla en störningsfri drift är det viktigt att begränsa tillträdet till driftmiljön. Installationer av tillträdesskydd, inbrottslarm och brandlarm ska göras enligt auktoriserad organisations normer. Tillträdeskontroll ska tillämpas för att säkerställa att endast behörig personal får tillträde.

9.1.1.1 Anvisningar för skalskydd och tillträde

9.1.1.1-1	Branschnormerna för brand- och stöldskydd ska följas. De normer som i första hand är aktuella heter: - EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia. - Svenska stöldskyddsföreningens norm (SSF) 200:5 (Regler för mekaniskt inbrottsskydd). - Telecommunications Infrastructure Standard for Data Centers (TIA) 942
9.1.1.1-2	Servrar och kommunikationsutrustning ska placeras i därför avsedda utrymmen.
9.1.1.1-3	Godkända lås- och larmsystem som är anpassade till aktuell driftmiljö ska finnas.
9.1.1.1-4	Observera att det alltid är försäkringsbolaget (eller annan kravställare) som godkänner säkerhetsprodukter (lås och larm). Av försäkringsvillkoren framgår vilka krav man ställer för att försäkringen ska gälla fullt ut. Kontrollera alltid vilka krav som gäller innan du väljer att köpa och montera nya säkerhetsprodukter.
9.1.1.1-5	Passerkontrollsystem ska finnas där känslig/sekretessbelagd information hanteras.
9.1.1.1-5	Nycklar och passerkort ska förvaras i säkerhetsskåp. Säkerhetsskåp ska uppfylla Stöldskyddsföreningens norm SS 3492.

9.1.1.1-6	Vid hantering av nycklar ska nyckelschema användas.
9.1.1.1-7	Extern eller egen personal, som inte har behörighet, får inte vistas ensamma i server- och kommunikationsutrymmen.
9.1.1.1-8	Vid externt besök i server- och kommunikationsutrymmen ska loggbok föras. I loggbok ska minst följande uppgifter noteras: - Besökarens namn och organisation/företag - Besöksmottagarens namn och organisatorisk tillhörighet - Tidpunkt för in- och utpassage - Syftet med besöket
9.1.1.1-9	I publika miljöer där det finns datorer ska det finnas inre och yttre skalskydd.
9.1.1.1-10	Skalskyddet kan bestå av larmade och låsta lokaler.
9.1.1.1-11	Datorer kan förses med vajerlås och förslagsvis låsas ihop parvis. Via låsbart bleck eller motsvarande kan datorn förankras mot det underlag den står på

9.2 Skydd av utrustning

Med informationsklassificering och riskanalys som grund ska åtgärder vidtas för att förhindra förlust eller skada på informationstillgångar och avbrott i verksamheten. Utrustning som tillhandahållits av arbetsgivaren ska behandlas på ett korrekt sätt.

9.2.1 FYSISKT SKYDD, ELFÖRSÖRJNING OCH KABLAGESKYDD

Beroende på placering av utrustningen krävs olika typer av fysiskt skydd.
Hänsyn ska tas till eventuella miljörisker.

9.2.1.1 Anvisningar för placering och skydd av utrustning

9.2.1.1-1	Brandskydd ska alltid finnas i eller i anslutning till server- och kommunikationsutrymmen.
9.2.1.1-2	Expertis skall alltid anlitas för att skapa rätt dimensionerat brandskydd. Följande punkter ska beaktas: - släckutrustning skall finnas i utrymmena och handsläckare i anslutning till utrymmena - rökdetektorer och därtill kopplat brandlarm skall finnas - genomföringar för ledningar och kablage skall vara brandtätade - dörrar till utrymmena skall vara brandklassade - nödbelysning bör finnas.
9.2.1.1-3	Verksamhetskritisk information/material ska förvaras i säkerhetsskåp i låst utrymme.
9.2.1.1-4	Arkivering av information lagrad på datamedia ska ske i rum eller skåp som uppfyller Riksarkivets krav enligt RA-FS 1997:3.

9.2.1.1-5	Den norm som i första hand är aktuell heter EN 1047 (EU norm för brandklassning) där brandklass P = för pappersdokument och brandklass DIS = för olika typer av datamedia.
9.2.1.1-6	Stöldbegärlig, dyr och svårersatt reservutrustning ska förvaras i låst utrymme med begränsat tillträde.
9.2.1.1-7	Stöldbegärlig utrustning ska om möjligt vara märkt.
9.2.1.1-8	Placering av skrivare och faxutrustning styrs av den typ av information som hanteras.
9.2.1.1-9	När känslig eller sekretessbelagd information skrivs ut ska utskriften övervakas eller skyddas.
9.2.1.1-10	Bärbar utrustning ska, när så är möjligt, vara utrustade med wirelås vid arbete utanför ordinarie arbetsplats. (Se även 9.2.2.1 Anvisningar för datorer i publik miljö)

9.2.1.2 Anvisningar för elförsörjning och kablageskydd

9.2.1.2-1	Verksamhetskritiska system och verksamhetsställen med starkt beroende av elförsörjning ska vara försedda med reservkraft.
9.2.1.2-2	Reservkraftsutrustningen ska testas regelbundet.
9.2.1.2-3	För att underlätta felsökning ska både kablar för strömförsörjning och datakommunikation dokumenteras på ritningar som ska hållas uppdaterade.

9.2.2 PUBLIKA MILJÖER

9.2.2.1 Anvisningar för datorer i publik miljö

De publika miljöer (medborgarkontor, bibliotek, skolor etc.) som staden tillhandahåller till stockholmarna har oftast IT-utrustning för informationssökning/-hantering.

9.2.2.1-1	På särskilt utsatta arbetsplatser ska utrustningen vara fastlåst.
9.2.2.1-2	I publika miljöer där datorer tillhandahålls ska det inre och yttre skalskyddet uppfylla stadens krav. (se 9.1.1.1 Anvisningar för skalskydd och tillträde)
9.2.2.1-3	I publika miljöer där datorer tillhandahålls och ingen åtkomstbegränsning är uppsatt ska ID-kort, lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.
9.2.2.1-4	Endast publika system ska kunna nås från datorn.
9.2.2.1-5	Det ska gå att förhindra åtkomst till webbsidor/-adresser (URL) med olämpligt innehåll och/eller skadlig påverkan genom filter mot surfning till olämpliga sidor. Respektive förvaltning/bolag beslutar själva vilka kategorier som ska exkluderas.

9.2.3 SÄKERHET FÖR UTRUSTNING UTANFÖR EGNA LOKALER

Utrustning som används utanför de egna lokalerna ska ha lika högt säkerhetsskydd som om den används i de egna lokalerna. Särskild hänsyn ska tas till risken för stöld och obehörig informationsåtkomst.

10 STYRNING AV KOMMUNIKATION OCH DRIFT

10.1 Driftrutiner och driftansvar

IT-chef eller motsvarande är ansvarig för ledning och drift av gemensamma informationstillgångar. Skriftlig driftdokumentation med ansvarsfördelning ska finnas.

10.1.1 DOKUMENTERADE DRIFTRUTINER

Driftrutinerna ska vara dokumenterade och hållas aktuella. Ändringsrutin för driftdokumentation ska tillämpas. I drift- och/eller förvaltningsåtagande för IT-system ska anvisningar finnas för att regelbundet kunna ta del av leverantörers systemrevisioner.

10.1.1.1 Anvisningar för driftdokumentation

För att kunna garantera kvaliteten i överenskommet IT-stöd krävs god ordning och aktuell driftdokumentation.

10.1.1.1-1	Dokumenterade driftrutiner med rutiner för åtgärder ska finnas
10.1.1.1-2	Originaldokumentationen ska förvaras i dokumentskåp som uppfyller Brandklass 90 P, godkänt av Statens Provningsanstalt.
10.1.1.1-3	Driftdokumentationen ska hållas aktuell och vara godkänd av tekniskt systemansvarig.
10.1.1.1-4	Det ska finnas en förteckning över all utrustning och programvara.

10.1.2 STYRNING AV ÄNDRINGAR I DRIFTMILJÖ

Ändringar i system som utbyter information med andra system ska beslutas i Stadens centrala ändringsråd (Change advisory board (CAB))

- Fastställda processer för hantering av förändringar i IT-system ska alltid följas.
- Process för ändringshantering ska följas även för åtgärder som är av rent infrastrukturell karaktär.
- Motsvarande process ska följas när det gäller IT-system som anskaffas från extern leverantör.
- Samtliga ändringar ska kunna härledas till en ansvarig beställare.

10.1.2.1 Anvisningar för ändringar i driftmiljö

Rutiner för ändringshantering minskar riskerna för driftstörningar.

10.1.2.1-1	Rutiner för ändringshantering (även för mindre ändringar) ska finnas etablerade inom systemets förvaltningsorganisation. Respektive systemägarrepresentant, såväl central som lokal, ansvarar för detta i samråd med driftteknisk personal.
10.1.2.1-2	Samtliga ändringar ska kunna härledas till en beställare.
10.1.2.1-3	All ändring av programvara ska godkännas innan den installeras i utbildnings-/produktionsmiljö. Innan installationen görs ska det finnas ett testprotokoll som är undertecknat av styrgrupp eller motsvarande. IT-handboken, del Testhandboken ska följas.

10.2 Systemplanering och systemgodkännande

Det ska finnas både en skriftlig rutin för driftgodkännande av IT-system och en rutin för bedömning av framtida kapacitetsbehov.

10.2.1 DRIFTGODKÄNNANDE

Driftgodkännande ska föregås av en definierad testfas. Ytterligare information finns i testhandboken.

10.2.1.1 Anvisningar för systemplanering och systemgodkännande

Innan driftsättning ska säkerhetskraven identifieras, värderas och beslutas.

10.2.1.1-1	Systemet ska vara driftgodkänt av styrgrupp eller motsvarande. Informationsklassificering typ B ska vara genomförd. Se IT-handboken.
10.2.1.1-2	Acceptanstestet ska beskrivas i projektets styrande dokument Testplan. I testplanen ska det anges under vilka förhållanden leveranstesten ska genomföras. Där ska t.ex. anges: - Teknisk miljö - Omfattning av testarbetet - Volymer av testdata - Antal användare och kategorier som ska testa - Användarnas förkunskaper - Faktorer som mäts Se vidare i Testhandboken
10.2.1.1-3	Service Level Agreement (SLA) som ingår i Drift- och förvaltningsavtal ska vara fastställt och kommunicerat till berörda parter.
10.2.1.1-4	Innan beslut fattas om att använda extern leverantör av IT ska riskanalys genomföras. Staden ska kontrollera hur avtalet tillämpas och hantera ändringar för att säkerställa att utförda tjänster uppfyller alla avtalade krav.
10.2.1.1-5	Alla krav på tjänsteleveranser ska regleras genom ett s.k. Service Level Agreement (SLA-avtal).

10.2.1.1-6	SLA-avtalet bör särskilt reglera följande: - Tjänstens tillgänglighetstider - Tjänstens användarkapacitet - Informationssäkerhet - Undantag - Förändringar i tjänsten - Tillåtna avbrott - Åtgärder vid avbrott - Backup - Dokumentation och statistik - Support - Mätning och uppföljning av SLA-uppfyllnad - Viten
10.2.1.1-7	Om tjänsten innehåller behandling av känsliga uppgifter, personuppgifter eller liknande ska särskilda krav om hur dessa ska hanteras ställas på leverantören.
10.2.1.1-8	Kapacitetsbehov/prestanda av lagringsutrymme, processorer etc. ska övervakas och följas upp.
10.2.1.1-9	Kontroll av filtyper, filstorlekar och liknande tekniska uppgifter ska utföras av tekniskt driftansvarig, med stickprov eller vid behov efter beställning från staden

10.3 Skadlig kod

Åtgärder för att upptäcka, förebygga och skydda mot skadlig programkod ska genomföras. Rutiner ska också finnas för hur användarna uppmärksammas på risker och regler.

10.3.1 SKYDD MOT SKADLIG KOD

Det ska gå att förhindra åtkomst till webbsidor/-adresser (URL) med skadlig påverkan och/eller olämpligt innehåll genom filter mot surfning till olämpliga sidor. Respektive förvaltning/bolag beslutar själva vilka kategorier som ska exkluderas

10.3.1.1 Anvisningar för åtgärder mot skadlig kod

Skadlig kod (virus, maskar, logiska bomber, trojaner, spionprogram etc.) innehåller funktioner som har till syfte att påverka datorer, kommunikation och information negativt.

10.3.1.1-1	Programvara för skydd mot skadlig kod ska installeras och kontinuerligt uppdateras på stadens datorer.
10.3.1.1-2	Alla stadens datorer, servrar och klienter, ska vara skyddade mot skadlig kod/ skadliga program.
10.3.1.1-3	Centralt avtalade produkter ska i möjligaste mån användas. Processen för att använda dessa hanteras av stadsledningskontoret.
10.3.1.1-4	Skyddet ska aktiveras automatiskt då datorn startas.

10.3.1.1-5	Uppdatering av antivirusskyddet ska utföras automatiskt vid anslutning till stadens nätverk. Om detta inte är möjligt ska manuell uppdatering ske regelbundet.
10.3.1.1-6	Programvara som installeras i stadens datorer ska vara certifierade (godkända av behörig beställare).
10.3.1.1-7	Nedladdning/lagring av programvaror och filer från okända eller tvivelaktiga webplatser är förbjudet.

10.3.1.2 Anvisningar för säkerhetsuppdateringar (patchar)

Säkerhetsuppdateringar ska alltid bedömas innan aktuell patch kan installeras.

10.3.2.1-1	Rutin ska finnas för att hantera leverantörers säkerhetsuppdateringar.
10.3.2.1-2	Nya virussignaturfiler ska installeras inom 24 timmar efter utgivning på samtliga servrar.
10.3.2.1-3	Relevanta utgivna säkerhetspatchar ska testas och installeras inom 7 dygn. Detta gäller såväl operativsystem som applikationer.

10.4 Säkerhetskopiering

Utrymme eller skåp som innehåller säkerhetskopior ska brandskyddas i enlighet med lagstiftningen samt normer från försäkringsinstitut. Kritiska säkerhetsfunktioner som återställning av säkerhetskopior ska övas och kontrolleras. Säkerhetskopiorna ska förvaras i annan byggnad än där systemet förvaras.

10.4.1 SÄKERHETSKOPIERING

Nivån och frekvensen på säkerhetskopiering av information ska definieras av systemägarrepresentant eller motsvarande. Säkerhetskopieringen ska schemaläggas, dokumenteras och utföras av behörig personal.

10.4.1.1 Anvisningar för säkerhetskopiering

Säkerhetskopiering (backup) innebär att filerna finns sparade i en kopia som senare kan återläsas om originalet skadas eller försvinner.

10.4.1.1-1	Alla användare ska upplysas om vad som säkerhetskopieras och hur de delar som inte säkerhetskopieras ska hanteras.
10.4.1.1-2	Säkerhetskopiering ska ske enligt vad som överenskommits i SLA/drift- och förvaltningsavtal. Det är respektive systemägarrepresentant som fastställer krav på frekvens av säkerhetskopiering, förvaringsplats för arkivkopia, krav på återläsningstid m.m.
10.4.1.1-3	Återläsning av säkerhetskopia ska testas regelbundet.
10.4.1.1-4	Datamedia ska förvaras i datamediaskåp eller motsvarande. Datamediaskåp ska uppfylla Brandklass 90 P, godkänt av Statens Provningsanstalt.

10.4.1.1-5	Säkerhetskopior ska förvaras i annan byggnad, minst 500 meter från platsen där systemet finns (eller om så inte är möjligt i annan brandcell än där systemet finns).

10.5 Styrning av nätverk

Skyddet av stadens egna nätverk för informationsöverföring ska skyddas utifrån verksamhetens krav och kopplingar mot externa datanät. Hantering av säkerheten för nätverk, som kan sträcka sig över organisationsgränserna, kräver särskilda åtgärder. Ytterligare åtgärder kan krävas för skyddet av känsliga data som sänds via allmänna nät.

- ansvar och anvisningar ska fastställas för hantering av all ingående utrustning i nätverk
- särskilda åtgärder avseende informationens behov av skydd gällande åtkomstbegränsning och
- riktighet när data passerar allmänna nät liksom skydd mot anslutna IT-system.

10.5.1 NÄTVERK

Anvisningar och instruktioner ska finnas för att uppnå och upprätthålla fastställd säkerhetsnivå i stadens nätverk.

10.5.1.1 Anvisningar för säkerhetsarkitektur i nätverk

Speciell hänsyn krävs vid kommunikation över organisationsgränser samt vid överföring av känslig information.

10.5.1.1-1	Information ska kunna överföras oförvanskad i nätverk
10.5.1.1-2	All extern (riktad till egen organisation) trafik baserad på TCP/IP ska gå via brandvägg och filtreras utifrån verksamhetsbehoven. Hänsyn måste tas till om det gäller åtkomst till stadens gemensamma resurser alternativt egen förvaltning/bolag/skola och vem som vill nå aktuell resurs (behörighetsaspekt). Generellt ska oönskad trafik vara spärrad
10.5.1.1-3	Följande grundfunktioner bör finnas i en brandvägg: - Paketfiltering (TCP/UDP portar, ip-adresser). - Tillståndsbaserad filtrering (autenticering). - NAT. - VPN funktionalitet. - VLAN hantering. - Övervakning av trafik (loggar).
10.5.1.1-4	Utgående Internettrafik ska passera stadens utpekade passeringspunkter (t.ex. proxyserver)
10.5.1.1-5	Intrångsdetekteringssystem (IDS) ska användas för att möjliggöra spårning av intrång och intrångsförsök i stadens informationssystem
10.5.1.1-6	Förvaltningar och bolag ska vara logiskt separerade från varandra

10.5.1.1-7	Portöppningar i brandväggar ska beslutas och dokumenteras av behörig beställare. Beslut om portöppning ska minst innehålla: syfte med portöppningen, beställare, tidsbegränsning och kontaktperson.
10.5.1.1-8	Det ska vara möjligt att separera nät fysiskt från varandra
10.5.1.1-9	Sammankoppling av nät hos t.ex. leverantör ska godkännas av staden
10.5.1.1-10	Systemklockor ska synkroniseras mot stadens NTP-server vilken i sin tur ska vara synkroniserad mot atomur.

Trådlösa nät (WLAN)

10.5.1.1-11	Innan ett trådlöst nätverk upprättas ska en bedömning ska göras om det är möjligt att uppnå samma effekt med ett trådbaserat nät. Säkerhetsarkitektur trådlösa nät: - WLAN ska alltid anslutas via brandvägg. - Autenticering ska alltid ske med certifikat eller engångslösenord. - Kontroller och penetrationstester ska ske regelbundet. - Nätverksnamnet ska inte annonseras via accesspunkten (AP). - Nätverksnamnet ska inte anknyta till verksamheten. - Accesspunkterna ska vara skalskyddade. - Access till Internet ska inte kunna ske utan inloggning. - IP-adresser via DHCP ska endast utdelas till kända klienter. - WLAN ska vara krypterade där så är möjligt med WPA-2.

10.6 Mediahantering och mediasäkerhet

10.6.1 HANTERING AV FLYTTBARA MEDIA

Som flyttbara media räknas CD-/DVD- skivor, usb-stickor, externa hårddiskar men också telefoner med inbyggd minnesenhet m.m.

10.6.1.1 Anvisningar för hantering av flyttbara media

Flyttbara media har stor lagringskapacitet och det kan medföra skada för staden om dessa kommer i orätta händer.

10.6.1.1-1	Flyttbara media som tas med utanför arbetsplatsen bör inte innehålla mer information än den som är absolut nödvändig.
10.6.1.1-2	Kopia av innehållet på flyttbart media som förs utanför arbetsplatsen ska finnas kvar på arbetsplatsen. Detta för att kunna bedöma skadan vid en förlust.
10.6.1.1-3	Användaren ansvarar för att känslig information krypteras

10.6.2 AVVECKLING AV MEDIA

Lagringsmedia ska förstöras eller raderas på ett säkert sätt. Av spårbarhetsskäl ska det dokumenteras hur känsligt material avvecklas.

10.6.2.1 Anvisningar för avveckling av media

Det är viktigt att förhindra att lagrad information kan användas i oönskat syfte.

10.6.2.1-1	Register ska upprättas för all media (band, disk etc.) där även förvaringsplatsen ska anges. Avyttring ska dokumenteras. Av dokumentationen ska framgå datum för avyttring, typ av information och till vem lagringsmediet har lämnats. Destruktionsintyg från destruktionsfirman eller leverantören som återtagit utrustningen ska arkiveras genom objektsförvaltare-IT eller motsvarande försorg.
10.6.2.1-2	Lagringsmedia som hanterat information med klassificeringsparameter 2 eller 3 för åtkomstbegränsning/sekretess får skrivas över med godkänt verktyg eller förstöras.
10.6.2.1-3	Lagringsmedia som hanterat information med klassificeringsparameter 1 för åtkomstbegränsning/sekretess får överskrivas och återanvändas i ”nivå 1 system” eller förstöras.
10.6.2.1-4	Vid avyttring av lagringsmedia med känsligt innehåll ska åtgärder vidtas så att informationsinnehållet görs oläsbart.
10.6.2.1-5	Destruktion ska ske på ett miljömässig korrekt sätt.

10.6.3 SÄKERHET FÖR SYSTEMDOKUMENTATION

Systemdokumentation ska skyddas i enlighet med aktuell säkerhetsprofil.

10.6.3.1 Anvisningar för systemdokumentation

10.6.3.1-1	Systemdokumentation ska skyddas i enlighet med den klassificering som gäller för aktuellt system.
10.6.3.1-2	Systemdokumentationen ska hållas aktuell och vara godkänd av systemförvaltare.

10.7 Utbyte av information och program

Vid informationsutbyte mellan organisationer ska gemensamma bedömningar göras av behovet av skydd mot åtkomst och riktighet samt krav på tillgänglighet. Ansvarsförhållanden ska vara klarlagda.

10.7.1 ANNAT INFORMATIONSUTBYTE

Informationsutbyte mellan staden och externa parter ska styras och upprättas enligt gemensamma bedömningar av behovet av skydd mot åtkomst och riktighet samt krav på tillgänglighet. Ansvarsförhållanden skall vara klarlagda.

10.7.1.1 Anvisningar för annat informationsutbyte

10.7.1.1-1	Telefonsamtal med känslig information ska ske där det inte kan avlyssnas.

10.7.1.1-2	Känslig information på whiteboard, blädderblock och motsvarande ska avlägsnas/förstöras efter avslutat möte.
10.7.1.1-3	Känslig information får inte skickas med fax.

10.8 Elektroniskt offentliggjord information

10.8.1.1 Anvisningar för elektroniskt offentliggjord information

Åtgärder ska vidtas för att skydda riktigheten i elektroniskt offentliggjord information.

10.8.1.1-1	Det ska finnas en formell process för godkännande innan information görs allmänt tillgänglig.
10.8.1.1-2	Det ska alltid finnas en ansvarig utgivare för webbsidor. Denne ansvarar för att rutiner upprättas och efterlevs.
10.8.1.1-3	Förvaltningar och bolag ansvarar för att information som publiceras av den egna verksamheten i gemensamma system är korrekt.
10.8.1.1-4	All publicering ska ske via en testmiljö, så kallad staging eller ”förhandsvisning”

10.9 Övervakning

10.9.1 LOGGAR

Kritiska och säkerhetsrelevanta händelser i drift och datakommunikation ska vara spårbara. Varje transaktion ska kunna knytas till den som utfört den. Detta ska i första hand åstadkommas med automatiska loggningsfunktioner. Alternativt redovisas händelser skriftligt. Loggning bör inriktas på drift-, transaktions- och säkerhetshändelser.

10.9.1.1 Anvisningar för logghantering

Behovet av loggning och uppföljning av loggar (analys) fastställs av systemägarrepresentanten efter verksamhetens behov samt genomförd informationsklassificering.

10.9.1.1-1	Varje användare ska ha en unik identifikation (användar-ID). Användar-ID ska kunna användas för att spåra aktiviteter kopplade till den ansvariga individen.
10.9.1.1-2	Loggning och analys av obehöriga åtkomstförsök till informationstillgångar (nätverk, information m.m.) ska genomföras regelbundet oavsett klassificeringsresultat.
10.9.1.1-3	Åtkomst till loggar styrs av informationsklassificering av systemet.
10.9.1.1-4	Loggar ska finnas så att aktiviteter utförda av personer med hög behörighet kan spåras.
10.9.1.1-5	Loggar ska skyddas mot radering, manipulation och obehörig åtkomst.

11 STYRNING AV ÅTKOMST

Åtkomst till IT-system och nätverk ska styras utifrån verksamhetsbehov och säkerhetskrav.

11.1 Verksamhetskrav på styrning av åtkomst

Den som har behov av åtkomst till informationstillgångar för att kunna utföra sina arbetsuppgifter ska tilldelas åtkomsträttigheter (behörigheter).
Systemadministratörer/-tekniker ska ha individuella användaridentiteter. Om det inte är möjligt ska manuell logg föras.

11.1.1 ÅTKOMST

Åtkomst/behörighet ska tilldelas formellt och endast efter behov samt följas upp regelbundet.
Den som använder Stockholms stads informationstillgångar på ett sätt som strider mot stadens regler kan bli föremål för en disciplinär åtgärd.

11.2 Styrning av användares åtkomst

Rutiner ska finnas för att säkerställa behöriga användares åtkomst och för att förhindra obehörigas åtkomst till stadens informationssystem.

11.2.1 BEHÖRIGHETSADMINISTRATION

Hantering av behörigheter ska ske enligt anvisningarna.

11.2.1.1 Anvisningar för hantering av behörighetsadministration

11.2.1.1-1	Behörighetsadministratörer ska finnas utsedda för stadens IT-system.
11.2.1.1-2	Verksamhetschef beslutar om aktuell behörighet.
11.2.1.1-3	**För tilldelning av behörigheter i centrala system gäller:** Beställning, signerad av verksamhetschef, med specificerade åtkomstkrav sänds till lokal behörighetsadministratör. Beställningen sänds sedan till den som är ansvarig för respektive behörighetskontrollsystem (vanligen driftleverantör). Driftleverantören ombesörjer uppläggning av identitet i det övergripande behörighetskontrollsystemet enligt beställningen. Övriga behörighetsbeställningar (till system i stordatormiljö) sänds till utsedda behörighetsadministratörer.
11.2.1.1-4	**För tilldelning av behörigheter i lokala nätverk och system gäller:** Beställningsrutiner för lokala system ska tas fram av respektive förvaltning och bolag med beaktande av delegations- och attestordning.

11.2.1.1-5	**För tilldelning av behörigheter utanför den egna förvaltningen gäller:** Vid behörighetstilldelning utanför egen förvaltning sänds beställning, efter signering av verksamhetschef, till systemförvaltare för aktuellt system. Denne stämmer av beställningen med systemägarrepresentanten och ombesörjer att behörighet tilldelas enligt ordinarie rutiner samt svarar även för att behörigheten avslutas efter ändring av befattnings- eller anställningsförhållanden eller motsvarande. På ansökan om behörighet ska därför alltid giltighetstid anges. Om informationsägare är annan än systemägaren ska denna underrättas.
11.2.1.1-6	Med lämpligt tidsintervall ska listor på samtliga behörigheter tas ut och kontrolleras. Intervallet avgörs av omfattningen på förändringar.
11.2.1.1-7	Genomgång av konton ska ske minst en gång per år. För grupper med höga behörigheter ska genomgång ske oftare. Kontroll ska göras av att kontoinnehavaren fortfarande arbetar och om arbetsuppgifterna har förändrats. Vid förändrade arbetsuppgifter behöver behörigheterna ses över.
11.2.1.1-8	Behörighetsadministratören ska omgående informeras om personal slutar sin anställning eller annan förändring som påverkar behörigheten sker.
11.2.1.1-9	**För vikarier och inhyrd personal ska tilldelning av behörigheter ske enligt separata instruktioner.** På arbetsplatser som anlitar inhyrd personal ska det finnas ett antal behörighetskonton som förvaras i slutna kuvert och inlåsta. Behörigheten ska sättas på en sådan nivå att det är möjligt att utföra arbetsuppgifter men ingenting mer. Antalet behörighetsnivåer vid en viss arbetsplats ska vara så få som möjligt så att administrationen blir enkel. För dessa specialkonstruerade vikariatsbehörigheter gäller följande: - Det ska bara gå att nå och arbeta i aktuell tillämpning. - Den ska bara gälla inom den del av organisationen, som uppdraget avser. - Lösenordet (i nät och tillämpning) ska bytas direkt när vikariatet går ut. - Byte av lösenord ska göras av berörd chef/arbetsledare alternativt systemförvaltare. - Id och lösenord ska förvaras på ett betryggande sätt (kassaskåp eller motsvarande) när de inte används. För att uppfylla stadens krav på att varje transaktion ska kunna knytas till den som utfört den, måste dessa i grunden anonyma behörigheter kompletteras med en manuell användarlogg. Den ska bestå av en lista där arbetsledaren antecknar att en viss behörighet använts av vikarie X under en viss tid. Vikarien ska också kvittera ut behörigheten i denna logg. Loggen ska förvaras under lås på samma sätt som kuverten med behörigheterna. Genom den manuella loggen blir det möjligt att i efterhand fastställa vem som vid en viss tidpunkt varit innehavare av en viss behörighet.

11.2.1.1-10	Tilldelning av behörigheter till personer med kommuncentrala arbetsuppgifter sker enligt systemägarrepresentantens instruktioner.

11.2.2 LÖSENORDSREGLER

Ett starkt lösenord innehåller alla sorters tecken; små bokstäver, stora bokstäver, siffror och specialtecken. Ju längre och komplexare lösenord, desto längre tid tar det att knäcka det.

- Välj aldrig ett lösenord som kan kopplas till dig på något sätt.
- Ha med alla typer av tecken i lösenordet, d v s små bokstäver, stora bokstäver, siffror och specialtecken.
- Om du måste skriva ner ditt lösenord, gör det på ett papper och behandla det som ett värdepapper.
- Ge aldrig ut ditt lösenord till någon annan.

Stockholms stads krav på lösenord:

1. Lösenordet ska innehålla minst åtta av följande tecken

OBS inte å ä ö Å Ä Ö

: ; < = > ? @ ! " # $ % & ' ( ) * + , { | } ~ . / [\ ] ^ _ `

0 1 2 4 5 6 7 8 9

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

a b c d e f g h i j k l m n o p q r s t u v w x y z

2. Lösenordet ska bestå av en blandning av tecken.
3. Användaren ska tvingas byta lösenord minst var 90:e dag.
4. Repeterbarhet av lösenord ska vara förhindrat i minst 13 generationer.
5. Låsning av användare p.g.a. inaktivitet ska ske efter 60 dagar där så medges.
6. Maximalt sex (6) felaktiga försök till inloggning ska vara tillåtet. Därefter låses användaridentiteten.

Stockholms stads krav på ”PIN”-kod:

En PIN-kod används på enheter som inte har tangentbord med bokstäver och siffror, t ex passersystem, mobiltelefoner och tjänstekort.

- Pinkoden skall bestå av minst 4 numeriska tecken.
- Godkända tecken är 0-9.
- Icke godkända kombinationer är:
  - Enkla sifferkombinationer, ex.vis 1111, 2222, 1234 etc.
  - Sifferkombinationer som på annat sätt är lätta att gissa sig till, t.ex. de fyra sista siffrorna i personnummer eller telefonknytning.
- Efter 3 (tre) misslyckade inloggningsförsök ska enheten låsas eller kontot inaktiveras

11.2.3 BEHÖRIGHETSKONTROLL

För användare ska åtkomst till informationstillgångar ske med ett behörighetskontrollsystem (BKS) där varje användare har en unik identitet och lösenord eller eventuellt en rolltillhörighet.

11.2.3.1 Anvisningar för behörighetskontroll

Behörighetskontrollsystem ska finnas och vara integrerade i de plattformar som väljs för serveroperativsystem, databashanterare och tillämpningar.

11.2.3.1-1	Lösenord och koder ska generellt vara individuella och får inte överlåtas eller lånas ut.
11.2.3.1-2	BKS ska vara integrerat i de plattformar som väljs för serveroperativsystem, databashanterare och tillämpningar. Undantag från den generella regeln kan förekomma men ska alltid hanteras i samråd med stadens informationssäkerhetschef. Möjlighet till spårbarhet ska alltid finnas.
11.2.3.1-3	SQL-, ODBC-, ADO (ActiveX Data Objects) -tjänster (m.fl.) får inte installeras så att IT-systemets databas kan anropas från klient utan att åtkomst prövas av tillämpade behörighetskontrollfunktioner.
11.2.3.1-4	För autenciering (identifiering) av användare får följande tekniker användas: - Certifikat eller elektroniskt id-kort - Biometrisk igenkänning - Lösenord
11.2.3.1-5	Lösenord ska skapas enligt gällande instruktioner.
11.2.3.1-6	I publika miljöer där datorer tillhandahålls ska id-kort, lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.

11.3 Styrning av åtkomst till nätverk

Interna och externa nätverk betraktas som informationstillgångar varför åtkomst styrs enligt samma principer som åtkomststyrning i övrigt. Stadens nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik.

11.3.1 UTNYTTJANDE AV NÄTVERKSTJÄNSTER

Rättighet att utnyttja olika former av nätverkstjänster ska beslutas och tilldelas enligt samma principer som åtkomststyrning i övrigt.

11.3.1.1 Anvisningar för nätverksanslutning

Datakommunikation är en kritisk resurs som kräver speciell fokus ur säkerhetssynpunkt.

11.3.1.1-1	En nätverksansluten persondator får inte samtidigt var ansluten till något annat nät (modem eller trådlöst).
11.3.1.1-2	All extern kommunikation mot stadens nätverk ska ske via IDportalen, eller VPN-lösning i speciella fall. Val av identifieringsätt styrs av den aktuella säkerhetsprofilen (via informationsklassificering).

11.3.1.1-3	All extern trafik (riktad till egen organisation) baserad på TCP/IP ska gå via brandvägg och filtreras utifrån verksamhetsbehov. (se Säkerhetsarkitektur nät 10.5.1.1)
11.3.1.1-4	För servicetjänster on-line ska avtal finnas med den part som har tillstånd till uppkopplingen.
11.3.1.1-5	Alla andra än av staden, för ändamålet, konfigurerade datorer som ansluts till stadens nätverk ska endast kunna komma åt internet på ett spårbart sätt
11.3.1.1-6	Användning av trådlösa nätverk (WLAN) ska ske restriktivt och baseras på verksamhetsbehov. (se Säkerhetsarkitektur nät 10.5.1.1)
11.3.1.1-7	Diagnosportar för distansunderhåll ska vara avstängda och fysiskt skyddade när de inte används. När diagnosporten behöver användas ska åtkomsten vara styrd från staden.

11.4 Styrning av åtkomst till operativsystem

Operativ- och behörighetskontrollsystem ska utformas och användas för att styra användares och administratörers åtkomst till informationstillgångar.

11.4.1 ÅTKOMST TILL OPERATIVSYSTEM

Rutinen för påloggning till ett operativsystem ska utformas så att möjligheterna till obehörig åtkomst minimeras.

11.4.1.1 Anvisningar för åtkomst till operativsystem

Restriktivitet ska gälla vid tilldelning av åtkomsträttigheter till operativsystem.

11.4.1.1-1	Operatörskonsolfunktion ska skyddas med stark autenciering.
11.4.1.1-2	Åtkomst till konsol ska skyddas med antingen certifikat eller engångslösenord.
11.4.1.1-3	Max fem inloggningsförsök ska tillåtas. Därefter ska användarkontot spärras.
11.4.1.1-4	Systemverktyg som kan förbigå system- och tillämpningsspärrar ska användas restriktivt, styras noga och endast användas av behörig systemadministratör.

11.5 Styrning av åtkomst till information och tillämpningar

Katalogstrukturer ska utgå från verksamhetens organisation och ansvarsförhållanden.

11.5.1 ÅTKOMST TILL INFORMATION OCH VERKSAMHETSSYSTEM

Systemägarrepresentanten har ansvaret för tilldelning av behörigheter i ett verksamhetssystem.

11.5.1.1 Anvisningar för åtkomst till information och verksamhetssystem

11.5.1.1-1	Systemägarrepresentanten ska besluta om ett IT-systems information ska vara åtkomlig från externa platser.
11.5.1.1-2	Alla användare som skapar eller tillför information i IT-system ska använda personliga användarkonton.
11.5.1.1-3	Max fem inloggningsförsök ska tillåtas. Därefter ska användarkontot spärras.
11.5.1.1-4	En rutin ska finnas för utlämnande av allmän handling där information hämtas från ett IT-system.
11.5.1.1-5	Utlämnandet kan ske genom utskrift, digitalkopia eller på bildskärm.
11.5.1.1-6	Allmänheten kan få använda en terminal om: - Det inte finns någon möjlighet att komma åt handlingar som inte är allmänna. - Det inte går att komma åt sekretessbelagda handlingar. - Det inte finnas någon risk att handlingarna förstörs eller ändras.

11.6 Mobil datoranvändning och distansarbete

Informationssäkerheten ska säkras vid användning av mobil utrustning och vid distansarbete.

11.6.1 MOBIL DATORANVÄNDNING

Med mobil datoranvändning avses:
”Åtkomstmöjlighet till stadens system utanför ordinarie arbetsplats”
Hänsyn måste alltid tas till risken att obehöriga kan ta del av medförd information.

11.6.1.1 Anvisningar för mobil datoranvändning

Mobil datoranvändning omfattar användning av bärbara PC, handdatorer, avancerade mobiltelefoner och andra liknande enheter från annan plats än arbetsplatsen. För att få åtkomst till program och data krävs säkerhetsmässigt godtagbara lösningar.

11.6.1.1-1	ADSL/3G-kommunikation/VPN eller annan säker lösning ska ske med hjälp av krypterat lösenordsutbyte mellan routrar.
11.6.1.1-2	De risker som finns med att använda trådlösa publika nätverk ska beaktas.
11.6.1.1-3	Uppkoppling mot stadens nätverk från publika miljöer ska ske via ID-portalen eller annan lösning som staden godkänt. Val av identifieringssätt styrs av säkerhetsprofilen som definieras vid informationsklassificeringen.
11.6.1.1-4	All lagrad information på intern minnesenhet ska krypteras. Stadens rekommenderade lösningar ska användas.
11.6.1.1-5	Vid lagring på extern minnesenhet ska informationsinnehållet avgöra krypteringsbehovet.

11.6.1.1-6	Virusskydd ska vara installerat och aktiverat på mobila enheter, om den tekniska plattformen stöder detta. Skyddet ska aktiveras automatiskt då enheten startas. Uppdatering av virusskyddet ska ske automatiskt vid anslutning till stadens nätverk. Om detta inte är möjligt ska manuell uppdatering ske varje dag. (se 11.3.1.1.Skydd mot skadlig kod)
11.6.1.1-7	Utrustningen ska låsas efter max 10 minuters inaktivitet om den tekniska plattformen medger detta.
11.6.1.1-8	Bärbar utrustning ska skyddas med lösenord/motsvarande. (se 11.2.2 Lösenordsregler)
11.6.1.1-9	Bärbar utrustning ska vara stöldskyddsmärkt. (se 7.1.1.1 Märkning av utrustning)
11.6.1.1-10	Registrering och säkerhetsinställningar ska göras av behörig tekniker innan utlämning av utrustning för mobil datoranvändning får ske.

11.6.2 DISTANSARBETE

Med distansarbete avses: ”Av arbetsgivaren tillhandahållen arbetsplats i hemmet.”
Distansarbete avtalas mellan staden och arbetstagaren.
Samma säkerhetsnivå ska gälla för distansarbetsplats som för ordinarie arbetsplats.

11.6.2.1 Anvisningar för distansarbetsplats

Dessa anvisningar gäller arbete i hemmet med utrustning och kommunikationsförbindelse som tillhandahållits av arbetsgivaren.

11.6.2.1-1	Privat utrustning får inte användas.
11.6.2.1-2	Utrustningen ska följa stadens anvisningar för standardisering av datorer.
11.6.2.1-3	Utrustning ska vara stöldskyddsmärkt.
11.6.2.1-4	Datorn ska låsas efter 10 minuters inaktivitet.
11.6.2.1-5	Utrustningen får endast användas av den anställde.
11.6.2.1-6	Information ska lagras på servern.
11.6.2.1-7	Samma säkerhetsnivå för säkerhetsuppdateringar och virusskydd ska finnas på distansarbetsplatsen som på den ordinarie arbetsplatsen. Skyddet ska aktiveras automatiskt då datorn startas.
11.6.2.1-8	ADSL-kommunikation eller motsvarande ska ske med hjälp av krypterat lösenordsutbyte mellan routrar

12 SYSTEMUTVECKLING/-INKÖP OCH SYSTEMUNDERHÅLL

Systemutveckling ska alltid ske i enlighet med fastställda modeller och metoder. För samtliga informationstillgångar ska säkerhetskraven sammanställas utifrån genomförd riskanalys och informationsklassificering.

12.1 Säkerhetskrav på IT-system

Stockholms stads säkerhetsdomän byggs i flera lager kring den information som ska skyddas.

Behörighetskontrollen ska identifiera och autentisera en användare samt styra åtkomsten till de delar i IT-systemet som användaren har behörighet att ta del av.
(se Anvisningar för behörighetskontroll 11.2.3.1)

Intrångsskyddet ska på ett kontrollerat sätt ge åtkomst till olika tjänster i ett IT-system, både från insidan och från utsidan av det skyddade IT-systemet. Det kan ske genom att tillåta, neka och/eller genom att omdirigera informationsflödet genom intrångsskyddet.
(se Nätverksanslutning 11.3.1.1)

Skyddet mot skadlig kod ska skydda IT-system mot sådan programkod som i någon form kan skada IT-systemets resurser genom att röja, förändra eller förstöra de uppgifter, filer och program som finns i systemen
(se Skadlig kod 10.3.1.1)

Säkerhetsloggningen gör att man i efterhand kan spåra händelser som är av betydelse för säkerheten i ett IT-system. Säkerhetsloggningen hanterar *alla* sådana händelser som är av betydelse för säkerheten i systemen, alltså även sådana händelser som kan uppstå i IT-systemets övriga säkerhetsfunktioner. (se Logghantering 10.9.1.1)

Intrångsdetektering innebär att *övervaka* och *bearbeta* sådana händelser som kan vara av betydelse för säkerheten i ett IT-system. Intrångsdetekteringen är tänkt att övervaka säkerhetsrelevanta händelser utanför IT-systemen. (se Säkerhetsarkitektur nätverk 10.5.1.1)

Säkerhetsfunktion	Sekretess	Tillgängligh.	Riktighet	Spårbarhet
Behörighetskontroll	X	X	X	
Säkerhetsloggning		X	X	X
Intrångsskydd	X	X	X	
Intrångsdetektering		X	X	X
Skydd m Skadlig kod	X	X	X	

Bilden visar säkerhetsdomänens koppling till informationssäkerhetens fyra hörnstenar: sekretess/åtkomstbegränsning, tillgänglighet, riktighet och spårbarhet.

Säkerhetskraven på IT-systemen redovisas också i Handbok informationsklassificering.

12.1.1 ANALYS OCH SPECIFIKATION AV SÄKERHETSKRAV

Säkerhetskraven ska vara uppfyllda innan driftgodkännande kan ges.

12.1.1.1 Anvisningar för informationssäkerhet vid utveckling och tillämpning av Internettjänster (E-tjänster)

12.1.1.1-1	I samband med utveckling av nya tillämpningar och/eller förändringar i befintliga tjänster ska möjligheten till användande av elektronisk identifiering prövas. Elektronisk identifiering stöder framför allt tre huvudfunktioner: Stark autentisering (säker inloggning) Elektronisk signatur (säker utfärdare) Kryptering (insynsskydd av information).
12.1.1.1-2	För information som är offentlig ska skydd finnas mot förvanskning och förlust. Särskild vikt ska läggas vid att koden i webb-tillämpningar är skyddad mot manipulation i syfte att förhindra SQL-injektioner och liknande angrepp.
12.1.1.1-3	Personuppgifter ska skyddas med enligt integritets- och sekretesskrav (jämför PUL). Datainspektionens allmänna råd ”Säkerhet för personuppgifter” ska följas.
12.1.1.1-4	Vid införande av nya tjänster på Internet ska alltid informationsklassificering genomföras för att fastställa val av identifieringssätt. (se Informationsklassificering 7.2.1.1)
12.1.1.1-5	Om informationsklassificeringen ger en säkerhetsprofil lika med 1 för någon av klassningsparametrarna Åtkomstbegränsning, Riktighet och Spårbarhet ska certifikat på kort (hårt certifikat) användas.
12.1.1.1-6	Om informationsklassificeringen ger en säkerhetsprofil lika med 2 för någon av klassningsparametrarna får elektronisk legitimation/BankID, engångslösenord med dosa (för stadens anställda) alternativt engångslösenord med SMS eller annan likvärdig metod (sk. Tvåfaktorautentisiering) användas.
12.1.1.1-7	Om informationsklassificeringen ger en säkerhetsprofil lika med 3 får användarnamn och lösenord användas såvida inte tjänsten ska vara allmänt tillgänglig.
12.1.1.1-8	Användarnamn och lösenord får inte skickas i klartext.
12.1.1.1-9	Användarnamn och lösenord ska skyddas mot obehörig avläsning och modifiering.
12.1.1.1-10	Systemet ska skydda mot att obehöriga kan utnyttja en inloggad eller tidigare inloggad session.

För mer detaljerad information hänvisas till Handbok för val av IDentifieringssätt vid extern inloggning via Internet, (HID).

12.2 Säkerhet i tillämpningar

Införda säkerhetsåtgärder ska verifieras och godkännas av Systemägarrepresentanten utifrån fastställda säkerhetskrav innan driftgodkännande.

12.2.1 INFORMATIONSKVALITET

Kontrollmekanismer ska finnas så att förväntad informationskvalitet garanteras.

12.2.1.1 Anvisningar för användardokumentation

12.2.1.1-1	Användardokumentationen ska utformas utifrån olika användarens kunskaper och behov.
12.2.1.1-2	Användardokumentationen ska finnas tillgänglig för alla användare.
12.2.1.1-3	Som alternativ/komplement bör användardokumentationen finnas tillgänglig ”online”.

12.2.2 ELEKTRONISK SIGNATUR

Om utställarens identitet måste garanteras vid informationsutbyte (t.ex. med en underskrift) ska rekommenderad teknisk lösning användas.

12.2.2.1 Anvisningar för elektronisk signering

12.2.2.1-1	Elektroniska signaturer kan användas i stället för handskrivna signaturer. De kan möjliggöra elektroniska, juridiskt bindande avtal, order, betalningar och så vidare vid bland annat e-handel mellan företag/organisationer.
12.2.2.1-2	Elektronisk signering ska ske med säkerhetsmässigt acceptabel teknik och förväntad juridisk acceptans.

12.3 Kryptering

12.3.1 KRYPTERINGSREGLER

- Stadens godkända programvara för kryptering ska användas.
- Nycklar och algoritm ska skyddas mot obehörig åtkomst och manipulation minst lika väl som den information kryptot avser att skydda.
- Möjligheten för obehöriga att ta del av information genom avlyssning ska beaktas.

12.3.1.1 Anvisningar för kryptering

12.3.1.1-1	Behovet av kryptering ska styras av informationens värde.
12.3.1.1-2	Rekommenderade metoder för kryptering ska användas. Dessa beskrivs i ITP.
12.3.1.1-3	Om informationsklassificeringen ger en säkerhetsprofil lika med 1 för klassningsparametern Åtkomstbegränsning ska informationen krypteras om den tekniska plattformen medget detta.

12.4 Säkerhet i databaser och program

12.4.1 STYRNING AV SÄKERHET I DATABASER OCH PROGRAM

Hantering av databaser och program ska ske enligt fastställd systemutvecklings-/förvaltningsmodell.

12.4.1.1 Anvisningar för hantering av testdata och program

12.4.1.1-1	Dokumenterat acceptanstest ska vara avslutat före driftgodkännande. Testhandboken beskriver detta mer ingående.
12.4.1.1-2	Fastställd ändringsrutin ska vara avslutad före ändringsgodkännande.
12.4.1.1-3	All programvara (ny/ändring) ska godkännas innan installation i produktionsmiljö. Det ska det finnas ett testprotokoll, undertecknat av systemägarrepresentant eller annan av honom/henne utsedd person innan installationen i produktionsmiljön. IT-handboken, del Testhandboken ska följas.

12.5 Skydd av testdata

All information i samband med systemutveckling och förvaltning ska skyddas enligt samma principer som övrig verksamhetsinformation.

Data i testmiljö får inte innehålla verkliga persondata.

- Kopiering av produktionsdata ska loggas för att vara spårbar.
- Kopiering får endast ske efter skriftlig beställning från projektledare/systemägarrepresentant/systemförvaltare och ska registreras i ärendehanteringssystem eller motsvarande

13 HANTERING AV INFORMATIONSSÄKERHETS-INCIDENTER

13.1 Säkerhetsincidenter och funktionsfel

13.1.1 RAPPORTERING

Incidenter och säkerhetsmässiga svagheter ska rapporteras snarast så att åtgärder för att minimera skada, åtgärda brister och utreda eventuell brottslighet kan påbörjas.

13.1.1.1 Anvisningar för incidenthantering

13.1.1.1-1	Det är viktigt att rapportera incidenter för att kunna bedöma vilka säkerhetsåtgärder som ska prioriteras. Incidentrapporteringen möjliggör att hotbildens relevans kan säkerställas och att satsningar görs på de viktigaste områdena. Exempel på incidenter som ska rapporteras är omfattande virusangrepp, intrång/intrångsförsök och manipulation/radering av information.
13.1.1.1-2	Alla användare ska rapportera informationssäkerhetsincidenter till informationssäkerhetssamordnaren som i sin tur rapporterar allvarliga händelser till stadens informationssäkerhetschef. Stadens verktyg för rapportering av incidenter ska användas. Respektive förvaltning/bolag avgör hur den praktiska hanteringen av verktyget ska ske.

14 KONTINUITETS- OCH AVBROTTSPLANERING

Kontinuitets- och avbrottsplanering är förmågan och beredskapen att hantera störningar/ avbrott i en organisations verksamhet.

Om en allvarlig störning/avbrott inträffar i en verksamhet kommer stora och speciella krav att ställas på den berörda personalen. Många svåra och snabba beslut måste fattas i en pressad arbetssituation. För att begränsa skadeverkningarna i verksamheten är det därför av avgörande betydelse att man i förväg har fastställt den organisation som ska fungera när hela eller delar av kontinuitetsplanen måste aktiveras. Informationen till personal, användare, kunder och massmedia måste prioriteras.

14.1 Kontinuitetsplanering

Kontinuitetsplaneringen omfattar åtgärder för att identifiera och minska risker. Förutom den allmänna riskbedömningsprocessen ska konsekvenserna av skadliga incidenter begränsas för att säkerställa att den information som krävs för att verksamheten ska kunna bedrivas är tillgänglig.
Konsekvenserna av störningar, allvarlig händelse och extraordinära händelser ska analyseras med hänsyn till inverkan på verksamheten. Kontinuitetsplaner ska upprättas och införas för att säkerställa att viktiga funktioner kan återställas inom rimlig tid och att verksamheten kan fortgå utan IT-stöd.

14.1.1 PROCESSEN KONTINUITETSPLANERING

Processen ska fokusera på den aktuella verksamhetens prioriterade åtaganden. Det innebär planering och förberedelser av åtgärder så att verksamheten kan upprätthållas trots att allvarliga störningar/avbrott har inträffat.

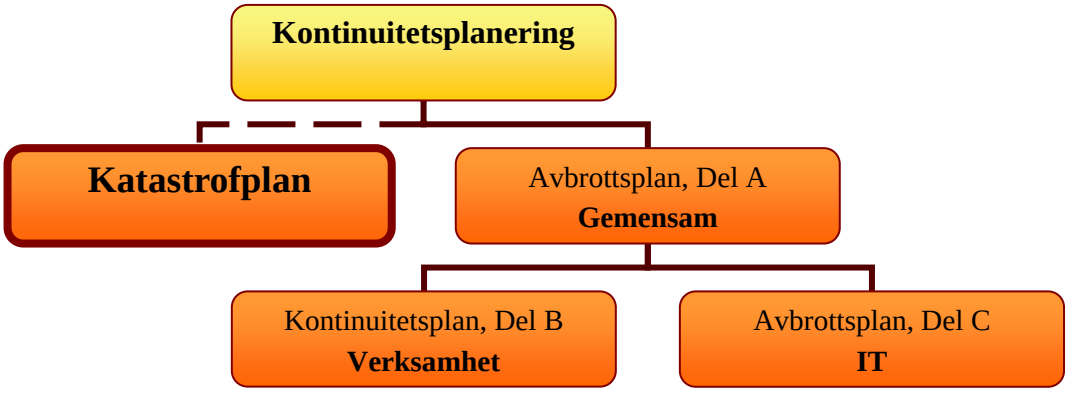
14.1.1.1 Anvisningar för processen kontinuitetsplanering

För att minska konsekvenserna vid allvarliga störningar/avbrott i verksamheter med starkt IT-beroende krävs en i förväg upprättad och dokumenterad kontinuitetsplan. Motsvarande planering för IT-verksamheten kallas avbrottsplanering.

14.1.1.1-1	Verksamhetsansvarig chef ansvarar för att det finns dokumenterad kontinuitetsplan för klassificerade system med Tillgänglighet nivå 1 eller 2 som används i verksamheten.
14.1.1.1-2	Kontinuitetsplanen ska omfatta: - Ansvar och befogenheter för kritiska rollinnehavare. - Informationskanalerna och vilka man informerar. - Reservplaner för olika händelser. - Plan för återgång till normalläge. - Plan för återtagning av förlorad information och annat av vikt. - Rutin för uppdatering av kontinuitetsplanen.
14.1.1.1-3	Det ska utses en ansvarig person för att hålla kontinuitetsplanen aktuell.
14.1.1.1-4	I SLA som ingår i drift- och förvaltningsavtal ska ansvaret för kontinuitetsplanen framgå. (se Anvisningar för systemplanering och systemgodkännande).

14.2 Avbrottsplanering

En avbrottsplan ska innehålla tre delar. Del A redovisar verksamhetens prioriterade åtaganden. Del B ska redovisa verksamhetsspecifika åtgärder och Del C redovisar vilka åtgärder IT-organisationen vidtar för att så snart som möjligt få tillbaka systemen i drift.



14.2.1 PROCESSEN AVBROTTSPLANERING

Processen ska fokusera på återstart av IT-systemen enligt fastställd prioritetsordning.

14.2.1.1 Anvisningar för processen avbrottsplanering

14.2.1.1-1	För att minska konsekvenserna vid allvarliga produktionsstopp krävs en avbrottsplan.
14.2.1.1-2	Den tekniskt systemansvarige ansvarar för att det finns en dokumenterad avbrottsplan om verksamheten använder klassificerade system med Tillgänglighet nivå 1 eller 2 och där maximal avbrottstid ska vara kortare än en vecka.
14.2.1.1-3	Avbrottsplanen ska omfatta: - Ansvar och befogenheter för kritiska rollinnehavare. - Informationskanaler och vilka man informerar. - Reservdriftalternativ. - Rutin för återstart. - Behov av utrustning/reservdelar. - Rutin för att uppdatera av avbrottsplanen.
14.2.1.1-4	Den tekniskt systemansvarige ansvarar för att hålla avbrottsplan del C aktuell.

14.3 Riskanalyser

14.3.1 PROCESSEN RISKANALYS

Processen ska fokusera på hoten mot den aktuella verksamhetens prioriterade åtaganden.

14.3.1.1 Anvisningar för processen riskanalys

14.3.1.1-1	Riskanalysen ska på ett systematiskt sätt granska och identifiera hot och risker i en verksamhet, bedöma konsekvenserna och ge åtgärdsförslag för att minimera hoten.
14.3.1.1-2	Riskanalys ska genomföras för klassificerade system nivå 1 eller 2.
14.3.1.1-3	Stadens rekommenderade metod ska användas.
14.3.1.1-4	Arbetsgången kan schematiskt beskrivas på följande sätt: - Identifiera hoten mot verksamheten. - Bedöma konsekvenserna om hoten förverkligas. - Fastställa vilken verksamhetsnivå som ska upprätthållas. - Ange vilka reservrutiner som behövs. - Prioritera återstartsordningen om flera system är berörda. Detta förutsätter en beskrivning av systemens inbördes samband. Beskrivning av stadens rekommenderade metoder återfinns i Handbok för RIskanalys, (HRI).
14.3.1.1-5	Deltagare i en riskanalys ska ha kunskap om och erfarenhet från den verksamhet som ska analyseras.

15 EFTERLEVNAD

En väl fungerande informationshantering bidrar till att staden kan fullgöra sina uppgifter. Det är därför viktigt att lagar och förordningar samt aktuella regelverk följs.

15.1 Identifiering av tillämpliga bestämmelser

15.1.1 LAGAR OCH FÖRORDNINGAR

Minimikraven för informationssäkerhet fastställs i lagar och förordningar.
Tryckfrihetsförordningen ställer krav på att allmänna handlingar ska vara tillgängliga medan offentlighets- och sekretesslagen inskränker på handlingars offentlighet.

Anvisningar för hantering av lagar och förordningar

15.1.1.1-1	Grundnivån för informationssäkerheten inom staden styrs bl.a. av lagar och förordningar. Här ges exempel på lagar som berör de flesta verksamhetsområden inom staden: - Tryckfrihetsförordningen (SFS 1949:105) - Offentlighets- och sekretesslagen (SFS 2009:400) - Säkerhetsskyddslagen (SFS 1996:627) - Lag om skydd för företagshemligheter (SFS 1990:409) - Bokföringslagen (SFS 1999:1078) - Lagen om kommunal redovisning (SFS 1997:614) - Arkivlagen (SFS 1990:782) - Personuppgiftslagen (SFS 1998:204) - Upphovsrättslagen (SFS 1960:729) - Lag om ansvar för elektroniska anslagstavlor (SFS 1998:112) - Lag om skydd för landskapsinformation (SFS 1993:1742)
15.1.1.1-2	Med stöd av Arkivnämndens allmänna anvisningar om gallring ska det beslutas vilka handlingar som kan gallras. Gallringsplaner ska upprättas och beroende på typ av handling anges vad som ska gallras och när det ska ske.

15.1.2 IMMATERIALRÄTT

Programvaror ska användas i enlighet med avtal och licensregler.

15.1.3 SKYDD AV PERSONUPPGIFTER

Data- och integritetsskyddet ska säkerställas enligt lagstiftningen och avtalsklausuler om sådana finns (t ex. samtycke). Detta ska även regleras med utomstående parter och externa leverantörer.
Hanteringen av personuppgifter i IT system ska dokumenteras och anmälas till personuppgiftsombud.

Detta sker bland annat i samband med informationsklassificeringen.

15.1.3.1 Anvisningar för system som hanterar skyddade identiteter (spärrmarkerade personuppgifter)

För att systemet med spärrmarkerade personuppgifter skall fungera är det viktigt att:

15.1.3.1-1	Personer med spärrmarkerade personuppgifter informeras om vikten av att inte i onödan lämna ut uppgifter om sig själva.
15.1.3.1-2	Spärrmarkeringar markeras tydligt vid sökningar i register.
15.1.3.1-3	Personal som hanterar personuppgifter informeras om sekretessfrågor och om systemet med spärrmarkerade personuppgifter.
15.1.3.1-4	Kretsen av personer som har behörigheten att ta del av spärrmarkerade personuppgifter begränsas så långt som möjligt.
15.1.3.1-5	Spärrmarkerade personuppgifter inte sprids till områden där sekretess för uppgifterna inte finns.
15.1.3.1-6	Efterlevnaden av rutinerna kring spärrmarkerade personuppgifter följs upp regelbundet.

15.2 Granskning av säkerhetspolicy, etik och teknisk efterlevnad

15.2.1 KONTROLL AV SÄKERHETSPOLICY OCH ETIK

Uppföljning av Internetanvändandet och användandet av stadens IT-system i övrigt ska göras för att kontrollera att regler och etiska normer efterlevs. Uppföljning i övrigt kan ske på olika sätt beroende på typ av verksamhet.

15.2.1.1 Anvisningar för säkerhetsuppföljning

15.2.1.1-1	Kontroll av enskilda personers surfning, e-post och lagrade filer kommer att ske då misstanke om brott eller missbruk föreligger.
15.2.1.1-2	Kontroll av enskild användares lagrade filer på den lokala hårddisken och i nätverket kan ske genom stickprov eller på annat vis. Kontrollen avser i första hand musik- och filmfiler, alltså inte vanliga Office-dokument.
15.2.1.1-3	Om kontrollerna ger upphov till misstankar om brott ska användaren ges tillfälle till förklaring. Därefter kan det bli aktuellt med polisanmälan.
15.2.1.1-4	Metodiken för att genomföra uppföljningar kan variera men några vanliga tillvägagångssätt är bland annat: - intern uppföljning med eller utan hjälp av IT-stöd - internrevision (oftast uppföljning av åtkomst, så kallad Auditing) - traditionell uppföljning/revision med hjälp av externa konsulter - attacksimulering/intrångsförsök av externa konsulter

15.2.1.1-5	Initiativtagare till säkerhetsuppföljningen kan vara informationssäkerhetschef, informationssäkerhetssamordnare eller verksamhetsansvarig chef
15.2.1.1-6	Kontinuerlig säkerhetsgranskning/revision ska genomföras.

15.2.2 KONTROLL AV TEKNISK EFTERLEVNAD

Den använda tekniken ska kontrolleras utifrån ett säkerhetsperspektiv. Exempelvis kan penetrationstester göras för att kontrollera IT-systemets åtkomst- och kommunikationsskydd.

15.3 Hänsynstaganden vid revision av IT-system

15.3.1 STYRNING AV REVISION AV IT-SYSTEM

IT-systeminriktad revision ska planeras, överenskommas och regelbundet genomföras för att minska risken för störningar i verksamhetsprocesserna.

Riktlinjerna för informationssäkerhetsarbetet ska granskas och revideras varje år för att se om betydande förändringar inträffat inom staden, för att säkerställa att dessa fortfarande är relevanta och inte står i strid med lagstiftningen och att riktlinjerna följer den tekniska utvecklingen. Ansvarig för att så sker är stadens säkerhetschef.

Stockholm den 4 december 2009

Irene Svenonius
Stadsdirektör